ROKIŠKIS

ROKIŠKIO RAJONO SAVIVALDYBĖS ADMINISTRACIJOS DIREKTORIUS

Į S A K Y M A S
DĖL ROKIŠKIO RAJONO SAVIVALDYBĖS INFORMACINĖS SISTEMOS TECHNOLOGIJŲ IR DUOMENŲ SAUGOS

2015 m. gruodžio 23 d. Nr. AV-1090
Rokiškis

Vadovaudamasis Lietuvos Respublikos vietos savivaldos įstatymo 29 straipsnio 8 dalies 2 punktu ir 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)“:

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

1.1. Rokiškio rajono savivaldybės informacinės sistemos duomenų saugumo nuostatus;

1.2. Rokiškio rajono savivaldybės informacinės sistemos naudotojų administravimo taisykles;

1.3. Saugaus elektroninės informacijos tvarkymo Rokiškio rajono savivaldybės informacinėje sistemoje taisykles;

1.4. Rokiškio rajono savivaldybės informacinės sistemos veiklos tęstinumo valdymo planą;

1.5. Rokiškio rajono savivaldybės kompiuterizuotos informacinės sistemos vartotojo instrukciją.

2. S k i r i u:

2.1. Rokiškio rajono savivaldybės administracijos Juridinio ir personalo skyriaus vyriausiąją specialistę Daivą Jasiūnienę Rokiškio rajono savivaldybės informacinės sistemos saugumo įgaliotinę;

2.2. Rokiškio rajono savivaldybės administracijos Ūkio tarnybos vyriausiuosius specialistus informatikai Daivą Ščerbickienę ir Igną Žilėną Rokiškio rajono savivaldybės informacinės sistemos administratoriais.

3. P r i p a ž į s t u netekusiu galios Rokiškio rajono savivaldybės administracijos direktoriaus 2009 m. kovo 2 d. įsakymą Nr. AV-151 „Dėl kompiuterių techninės ir programinės įrangos naudojimo Rokiškio rajono savivaldybės administracijoje tvarkos aprašo patvirtinimo“.

Šis įsakymas gali būti skundžiamas Lietuvos Respublikos administracinių bylų teisenos įstatymo nustatyta tvarka.

Administracijos direktorius Valerijus Rancevas

Daiva Jasiūnienė

PATVIRTINTA
Rokiškio rajono savivaldybės administracijos
direktoriaus 2015 m. gruodžio 23 d.
įsakymu Nr. AV-1090

ROKIŠKIO RAJONO SAVIVALDYBĖS INFORMACINĖS SISTEMOS DUOMENŲ SAUGUMO NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Rokiškio rajono savivaldybės (toliau – Savivaldybė) informacinės sistemos duomenų saugumo nuostatai (toliau – saugumo nuostatai) reglamentuoja Savivaldybės informacinės sistemos (toliau – informacinė sistema) duomenų saugumą ir nustato informacinės sistemos saugumo politiką.

2. Saugumo nuostatų tikslas – užtikrinti informacinėje sistemoje tvarkomų duomenų konfidencialumą, prieinamumą, vientisumą ir tinkamą kompiuterizuotų darbo vietų bei kompiuterių tinklo įrangos funkcionavimą.

3. Saugumo nuostatuose vartojamos sąvokos:

Elektroninė informacija (toliau – informacija) – visa informacija, kuri tvarkoma informacinių technologijų priemonėmis.

Informacijos saugumo įvykis (toliau – saugumo įvykis) – nustatytas sistemos, tarnybos ar tinklo įvykis, rodantis, kad yra galima saugumo užtikrinimo spraga ar apsaugos priemonių trikdis arba anksčiau nenumatyta situacija, kuri gali būti svarbi saugumui.

Informacijos saugumo incidentas (toliau – saugumo incidentas) – vienas ar daugiau nepageidaujamų ir netikėtų saugumo įvykių, turinčių didelę tikimybę pakenkti veiklai ir keliančių grėsmę informacijos saugumui.

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

Informacijos tvarkymas – visos su informacija atliekamos operacijos: rinkimas, kaupimas, saugojimas, keitimas, kopijavimas, sujungimas, atskleidimas, teikimas, naudojimas, naikinimas naudojant informacines technologijas.

Kitos saugumo nuostatuose vartojamos sąvokos suprantamos taip, kaip saugų duomenų tvarkymą reglamentuojančiuose Lietuvos Respublikos teisės aktuose, Lietuvos bei tarptautiniuose standartuose.

4. Informacijos saugumo užtikrinimo prioritetinės kryptys:

4.1. informacijos konfidencialumo užtikrinimas;

4.2. informacijos vientisumo užtikrinimas;

4.3. informacijos prieinamumo užtikrinimas;

4.4. informacinės sistemos veiklos tęstinumas;

4.5. asmens duomenų apsauga.

5. Informacinės sistemos valdytoja ir tvarkytoja yra Savivaldybės administracija, adresas Respublikos g. 94, LT-42136 Rokiškis.

6. Savivaldybės administracija, kaip informacinės sistemos valdytoja ir tvarkytoja:

6.1. atsako už informacinėje sistemoje tvarkomos informacijos tvarkymo teisėtumą ir informacijos saugumą;

6.2. rengia dokumentus, susijusius su informacinės sistemos saugumo užtikrinimu;

6.3. užtikrina nepertraukiamą informacinės sistemos veikimą ir duomenų, esančių informacinės sistemos duomenų bazėse, saugumą ir saugų duomenų perdavimą kompiuterių tinklais (automatiniu būdu);

6.4. tobulina informacinę sistemą ir informacinės sistemos duomenų saugumą;

6.5. organizuoja informacinės sistemos rizikos vertinimą;

6.6. vykdo informacinę sistemą sudarančių informacinių išteklių inventorizaciją;

6.7. atlieka kitas saugumo nuostatuose ir kituose teisės aktuose numatytas funkcijas.

7. Informacijos tvarkytojai yra Savivaldybės administracijos padaliniai, atsakingi už jiems priskirtos informacijos tvarkymą, priežiūrą ir saugumą.

8. Informacijos tvarkytojai atlieka šias funkcijas:

8.1. tvarko informaciją pagal jų veiklą reglamentuojančių įstatymų ir kitų teisės aktų reikalavimus;

8.2. teikia informaciją duomenų gavėjams;

8.3. vykdo saugumo dokumentuose nustatytus reikalavimus ir užtikrina tinkamą duomenų saugumą;

8.4. teikia pranešimus apie saugumo įvykius;

8.5. atlieka kitas saugumo nuostatuose ir kituose teisės aktuose numatytas funkcijas.

9. Savivaldybės administracijos direktorius skiria informacinės sistemos saugumo įgaliotinį (toliau – saugumo įgaliotinis) ir informacinės sistemos administratorių arba kelis administratorius, vykdančius atskiras informacinės sistemos administravimo funkcijas (toliau – administratorius).

10. Saugumo įgaliotinis, įgyvendindamas informacijos saugumą, atlieka šias funkcijas:

10.1. teikia siūlymus dėl saugumo dokumentų priėmimo, keitimo ar panaikinimo;

10.2. dalyvauja saugumo įvykių, įvykusių informacinėje sistemoje, tyrime;

10.3. konsultuoja naudotojus informacijos saugumo klausimais;

10.4. atlieka kitas saugumo nuostatuose ir kituose teisės aktuose numatytas funkcijas.

11. Administratorius atlieka tokias funkcijas:

11.1. naudotojams suteikia teisę naudotis informacija ir kompiuteriu paskirtoms funkcijoms atlikti;

11.2. administruoja serverius, kompiuterių tinklo įrangą, interneto svetainės veikimą, pašto ir paieškos sistemas, nustato pažeidžiamų vietų ir saugumo reikalavimų atitiktį;

11.3. registruoja saugumo įvykius, informuoja apie juos savo tiesioginį vadovą, teikia pasiūlymus dėl įvykį sukėlusių priežasčių pašalinimo;

11.4. atlieka kitas saugumo nuostatuose ir kituose teisės aktuose numatytas funkcijas.

12. Informacinės sistemos saugumo politiką įgyvendinantys dokumentai yra Saugaus elektroninės informacijos tvarkymo Rokiškio rajono savivaldybės informacinėje sistemoje taisyklės, Rokiškio rajono savivaldybės informacinės sistemos veiklos tęstinumo valdymo planas ir Rokiškio rajono savivaldybės informacinės sistemos naudotojų administravimo taisyklės (toliau – saugumo politiką įgyvendinantys dokumentai).

13. Savivaldybės informacinės sistemos saugumas užtikrinamas 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)“, kitais Lietuvos bei tarptautiniais standartais, reglamentuojančiais informacijos saugumą.

II. INFORMACIJOS SAUGUMO VALDYMAS

14. Pagrindiniai informacijos saugumo priemonių parinkimo principai yra šie:

14.1. rizika turi būti sumažinta iki priimtino lygio;

14.2. informacijos saugumo priemonės diegimo kaina adekvati saugomos informacijos vertei;

14.3. kur galima, turi būti įdiegtos prevencinės informacijos saugumo priemonės.

15. Asmens duomenų apsauga turi būti užtikrinta vadovaujantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu ir Savivaldybės administracijos direktoriaus patvirtintomis Asmens duomenų tvarkymo taisyklėmis.

16. Informacinėje sistemoje įvykusių saugumo incidentų valdymas ir informacinės sistemos veiklos atkūrimas vykdomas Rokiškio rajono savivaldybės informacinės sistemos veiklos tęstinumo valdymo plane nustatyta tvarka.

17. Siekiant užtikrinti šiuose saugumo nuostatuose ir kituose saugumo politiką įgyvendinančiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, ne rečiau kaip kartą per metus:

17.1. inventorizuojama informacinės sistemos techninė ir programinė įranga;

17.2. sudaromas informacinės sistemos informacinių išteklių sąrašas;

17.3. tikrinamas ir atnaujinamas Rokiškio rajono savivaldybės informacinės sistemos veiklos atkūrimo detalusis planas.

18. Techninės, administracinės ir kitos duomenų saugumo valdymo priemonės turi būti pasirenkamos taip, kad su kuo mažesnėmis išlaidomis būtų užtikrintas informacinės sistemos veiklos tęstinumas ir saugus naudotojų darbas.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

19. Naudotojų prieigos prie informacinės sistemos suteikimo tvarka nustatyta Rokiškio rajono savivaldybės informacinės sistemos naudotojų administravimo taisyklėse.

20. Prieiga naudotojams suteikiama tik prie tų išteklių, kurie yra būtini tiesioginėms pareigoms atlikti.

21. Naudotojų naudojama kompiuterinė technika skirta tik naudotojų tiesioginėms pareigoms atlikti.

22. Naudotojams draudžiama patiems diegti bet kokią programinę įrangą. Programinę įrangą, reikalingą naudotojo funkcijoms atlikti, diegia ir prižiūri Ūkio tarnybos darbuotojas.

23. Naudotojams gali būti suteikiama nuotolinio prisijungimo prie informacinės sistemos galimybė.

24. Nuotoliniam prisijungimui prie informacinės sistemos taikomi saugumo reikalavimai turi būti ne žemesni, nei taikomi prisijungimui prie vidinio Savivaldybės kompiuterių tinklo.

25. Serveriuose ir naudotojų kompiuteriuose turi būti naudojama programinė įranga, skirta apsaugoti informacinę sistemą nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.) (toliau – antivirusinė programinė įranga). Antivirusinė programinė įranga turi būti atnaujinama kiekvieną dieną.

26. Savivaldybės kompiuterių tinklas turi būti užkarda atskirtas nuo viešųjų telekomunikacijų tinklų.

27. Duomenų kopijų darymo tvarka nustatyta Saugaus elektroninės informacijos tvarkymo Rokiškio rajono savivaldybės informacinėje sistemoje taisyklėse.

28. Duomenys automatiniu būdu gali būti teikiami ir (ar) gaunami tik laikantis duomenų teikimo ir (ar) gavimo sutartyse nustatytos tvarkos arba teisės aktuose numatytais atvejais.

IV. REIKALAVIMAI PERSONALUI

29. Naudotojai privalo rūpintis tvarkomos informacijos saugumu.

30. Naudotojai turi būti susipažinę su šiais saugumo nuostatais ir saugumo politiką įgyvendinančiais dokumentais.

31. Saugumo įgaliotinis privalo išmanyti informacijos saugumo užtikrinimo principus, savo darbe vadovautis teisės aktais, standartais ir kitais su informacijos saugumu susijusiais dokumentais, reglamentuojančiais saugų informacijos tvarkymą.

32. Administratorius privalo išmanyti informacijos saugumo principus, darbą su kompiuterių tinklais, mokėti užtikrinti jų saugumą, taip pat administruoti ir prižiūrėti duomenų bazes, turi būti susipažinęs su saugumo nuostatais ir saugumo politiką įgyvendinančiais dokumentais.

33. Naudotojai turi turėti kvalifikaciją (informacinių technologijų naudotojų kvalifikacijos kursai, pradinis saugaus darbo su informacija mokymas, ECDL (Europos kompiuterio naudotojo pažymėjimas), naudotojo sertifikatas ar pan.) ir patirties dirbant su atitinkamomis operacinėmis sistemomis ir taikomosiomis programomis.

34. Juridinis ir personalo skyrius organizuoja naudotojų mokymus duomenų saugumo klausimais.

V. NAUDOTOJŲ SUPAŽINDINIMAS SU SAUGUMO DOKUMENTAIS

35. Už naudotojų supažindinimą pasirašytinai su šiais saugumo nuostatais, saugumo politiką įgyvendinančiais dokumentais ir atsakomybe už juose nustatytų reikalavimų nesilaikymą yra atsakingi Savivaldybės administracijos padalinių vadovai.

VI. BAIGIAMOSIOS NUOSTATOS

36. Saugumo nuostatai yra privalomi saugumo įgaliotiniui, administratoriui ir naudotojams.

37. Naudotojai, pažeidę šių saugumo nuostatų ar saugumo politiką įgyvendinančių dokumentų reikalavimus, atsako teisės aktų nustatyta tvarka.

PATVIRTINTA
Rokiškio rajono savivaldybės administracijos
direktoriaus 2015 m. gruodžio 23 d.
įsakymu Nr. AV-1090

ROKIŠKIO RAJONO SAVIVALDYBĖS INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Rokiškio rajono savivaldybės (toliau – Savivaldybė) informacinės sistemos (toliau – informacinė sistema) naudotojų administravimo taisyklės (toliau – Naudotojų administravimo taisyklės) nustato informacinės sistemos naudotojų įgaliojimus, teises, pareigas, supažindinimo su saugumo dokumentais ir saugaus informacinės sistemos duomenų teikimo informacinės sistemos naudotojams kontrolės tvarką.

2. Naudotojų administravimo taisyklėse vartojamos sąvokos:

Informacinės sistemos administratorius (toliau – administratorius) – Savivaldybės administracijos (toliau – Administracija) direktoriaus įsakymu paskirtas valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, atsakingas už naudotojų registravimą, prieigos teisių suteikimą ir panaikinimą, atliekantis kitas jam priskirtas funkcijas, aprašytas informacinės sistemos veiklą reglamentuojančiuose dokumentuose.

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

3. Kitos Naudotojų administravimo 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.

4. Naudotojų administravimo taisyklės taikomos informacinės sistemos administratoriui ir visiems naudotojams.

5. Prieinamumo prie informacinės sistemos duomenų principas – prieigos prie informacinės sistemos duomenų teisė suteikiama naudotojui tik tuo atveju, jei jam pavesta tvarkyti informacinės sistemos duomenis arba jam priskirtoms funkcijoms atlikti būtina naudotis informacinės sistemos duomenimis. Prieigos teisė prie viešai skelbiamų informacinės sistemos duomenų suteikiama visiems naudotojams.

II. NAUDOTOJŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

6. Naudotojai gali naudotis tik tais informacinės sistemos ištekliais, prie kurių prieigos teisę jiems suteikė administratorius.

7. Naudotojai privalo užtikrinti jų naudojamų informacinės sistemos saugomų ir apdorojamų duomenų konfidencialumą ir vientisumą, savo veiksmais netrikdyti duomenų prieinamumo.

8. Naudotojai turi teisę gauti informaciją apie jų naudojamų duomenų apsaugos lygį ir taikomas apsaugos priemones, rekomenduoti papildomas apsaugos priemones.

9. Kiti naudotojų įgaliojimai, teisės ir pareigos yra nustatyti Rokiškio rajono savivaldybės informacinės sistemos duomenų saugumo nuostatuose ir kituose informacinės sistemos saugumo politiką įgyvendinančiuose dokumentuose.

III. SAUGAUS DUOMENŲ TEIKIMO NAUDOTOJAMS KONTROLĖS TVARKA

10. Administratorius yra atsakingas už naudotojų registravimą, išregistravimą, prieigos prie informacinės sistemos teisių suteikimą, sustabdymą, sustabdymo panaikinimą ir prieigos prie

informacinės sistemos teisių panaikinimą.

11. Administratorius naudotojams suteikia unikalų prisijungimo prie informacinės sistemos vardą ir laikiną slaptažodį. Administracijos darbuotojas, paruošęs naudotojo kompiuterizuotą darbo vietą, perduoda jam prisijungimo prie informacinės sistemos vardą ir slaptažodį bei informuoja naudotoją apie tai, kad pirmą kartą prisijungęs prie informacinės sistemos naudotojas privalo pasikeisti gautą slaptažodį.

12. Prisijungimo prie informacinės sistemos slaptažodžių sudarymo, galiojimo trukmės ir keitimo reikalavimai yra šie:

12.1. naudotojų prisijungimo prie informacinės sistemos vardai ir slaptažodžiai saugomi naudotojų prisijungimo vardų ir slaptažodžių duomenų bazėje;

12.2. visiems naudotojams turi būti nustatomas slaptažodis, kuris formuojamas iš ne mažiau kaip 7 simbolių;

12.3. naudotojai privalo prisijungimo prie informacinės sistemos slaptažodį keisti ne rečiau kaip 1 kartą per metus;

12.4. draudžiama slaptažodžius atskleisti tretiesiems asmenims.

13. Naudotojų prieigos teisė naudotis informacine sistema privalo būti panaikinama:

13.1. gavus Administracijos direktoriaus įsakymą, Savivaldybės mero potvarkį dėl darbuotojo atleidimo;

13.2. Savivaldybės tarybos nariui netekus Savivaldybės tarybos nario įgaliojimų.

14. Baigus darbą su informacine sistema, turi būti atsijungiama nuo informacinės sistemos arba įjungiama ekrano užsklanda su slaptažodžiu.

15. Prisijungimas ir (ar) bandymas prisijungti prie informacinės sistemos automatiniu būdu įrašomi informacinės sistemos veiksmų žurnale, kuriame registruojama prisijungimo ir (ar) bandymo prisijungti data, prisijungimo trukmė.

16. Pricigos prie informacinės sistemos teisių suteikimo, sustabdymo, sustabdymo panaikinimo ir prieigos teisių panaikinimo tvarka:

16.1. Administracijos Juridinis ir personalo skyrius ir Kontrolės ir audito tarnyba teikia administratoriui kompiuterines dokumentų kopijas apie darbuotojų priėmimą, perkėlimą, atleidimą, Savivaldybės tarybos narių įgaliojimų pradžią ir pabaigą, Savivaldybės tarybos narių ar darbuotojų vardo ar pavardės pakeitimą.

16.2. Administratorius, gavęs Administracijos direktoriaus įsakymą, Savivaldybės mero potvarkį arba Kontrolės ir audito tarnybos informaciją apie naudotojo išvykimą ilgesniam kaip 2 mėnesių laikotarpiui (atostogos, komandiruotės ir kt.), pirmąją naudotojų išvykimo dieną sustabdo naudotojo prieigos teises, išskyrus prieigą prie elektroninio pašto, o naudotojų prieigos teisių sustabdymą panaikina pirmąją naudotojo darbo dieną jam parvykus.

16.3. Kai naudotojas perkeliamas į kitas pareigas, administratorius pakeičia jam suteiktas naudotojo prieigos teises.

16.4. Administratorius per 3 darbo dienas panaikina naudotojo prieigos teises 13 punkte nustatytais atvejais.

IV. NAUDOTOJŲ SUPAŽINDINIMO SU ROKIŠKIO RAJONO SAVIVALDYBĖS INFORMACINĖS SISTEMOS DUOMENŲ SAUGUMO NUOSTATAIS IR INFORMACINĖS SISTEMOS SAUGUMO POLITIKĄ ĮGYVENDINANČIAIS DOKUMENTAIS TVARKA

17. Naudotojai supažindinami su informacinės sistemos duomenų saugumo nuostatais ir informacinės sistemos saugumo politiką įgyvendinančiais dokumentais Rokiškio rajono savivaldybės informacinės sistemos saugumo nuostatuose nustatyta tvarka.

18. Visi naudotojai turi būti pasirašę Administracijos direktoriaus įsakymu patvirtintą Rokiškio rajono savivaldybės kompiuterizuotos informacinės sistemos vartotojo instrukciją.

19. Pasirašytos instrukcijos saugomos Administracijos Juridiniame ir personalo skyriuje.

PATVIRTINTA
Rokiškio rajono savivaldybės administracijos
direktoriaus 2015 m. gruodžio 23 d.
įsakymu Nr. AV-1090

SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO ROKIŠKIO RAJONO SAVIVALDYBĖS INFORMACINĖJE SISTEMOJE TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Saugaus elektroninės informacijos tvarkymo Rokiškio rajono savivaldybės (toliau – Savivaldybė) 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 (Žin., 1996, Nr. 63-1479; 2008, Nr. 22-804).

3. Tvarkymo taisyklėse vartojamos sąvokos:

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.

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

4. Kompiuterinės įrangos saugumo priemonės:

4.1. 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.

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

4.3. Yra įgyvendintos gamintojo nustatytos kompiuterinės įrangos darbo sąlygos.

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

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

5.1. Naudojama legali sisteminė ir taikomoji programinė įranga.

5.2. Programinės įrangos diegimą, konfigūravimą ir šalinimą atlieka tik Administracijos Ūkio tarnybos darbuotojai.

5.3. Programinė įranga prižiūrima laikantis gamintojo rekomendacijų.

5.4. Programinei įrangai ir duomenims apsaugoti naudojamos programinės priemonės: tinklo užkardos ir kompiuterinės aplinkos teisių sistema.

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

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

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

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

6.4. Įrengta bendro naudojimo patalpų durų fizinė apsauga.

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

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

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

7.2. 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.

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

III. SAUGUS INFORMACIJOS TVARKYMAS

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

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

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

11. Informacinės sistemos naudotojų veiksmų registravimas:

11.1. 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.

11.2. 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.

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

11.4. 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.

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

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

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

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

13.2. 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.

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

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

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

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

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

14.1. 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.

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

14.3. 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.

15. Prieš atlikdamas informacinės sistemos programinės ir techninės įrangos keitimą, kurio metu gali iškilti grėsmė duomenų ir informacinės sistemos konfidencialumui, vientisumui ar pasiekiamumui, sistemos administratorius pagal informacinės sistemos galimybes turėtų išbandyti planuojamus informacinės sistemos pokyčius.

16. 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

17. 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.

18. 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.

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

19.1. 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;

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

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

21. 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.

PATVIRTINTA
Rokiškio rajono savivaldybės administracijos
direktoriaus 2015 m. gruodžio 23 d. įsakymu
Nr. AV-1090

ROKIŠKIO RAJONO SAVIVALDYBĖS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS

I. BENDROSIOS NUOSTATOS

1. Rokiškio rajono savivaldybės (toliau – Savivaldybė) informacinės sistemos (toliau – informacinė sistema) veiklos tęstinumo valdymo plano (toliau – Valdymo planas) tikslas – nustatyti Savivaldybės administracijos (toliau – Administracija) darbuotojų veiksmus, informacinėje sistemoje esant elektroninės informacijos saugumo incidentui, kurio metu gali kilti pavojus informacinės sistemos techninės, programinės įrangos funkcionavimui ir duomenims.

2. Valdymo planas parengtas 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.

3. Valdymo plane vartojamos sąvokos:

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

Informacijos saugumo įvykis (toliau – saugumo įvykis) – nustatytas sistemos, tarnybos ar tinklo įvykis, rodantis, kad yra galima informacijos saugumo užtikrinimo spraga ar apsaugos priemonių trikdis arba anksčiau nenumatyta situacija, kuri gali būti svarbi saugumui.

Informacijos saugumo incidentas (toliau – saugumo incidentas) – vienas ar daugiau nepageidaujamų ir netikėtų saugumo įvykių, turinčių didelę tikimybę pakenkti veiklai ir keliančių grėsmę informacijos saugumui.

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

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

Informacinės sistemos naudotojai (toliau – naudotojai) – Savivaldybės tarybos nariai, Savivaldybės tarybos sekretoriato, Savivaldybės kontrolės ir audito tarnybos, Administracijos valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartį.

Informacinės sistemos veiklos tęstinumas – gebėjimas nenutrūkstamai vykdyti informacinės sistemos veiklą.

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

4. Valdymo planas įsigalioja, kai dėl įvykių, nurodytų Rokiškio rajono savivaldybės informacinės sistemos veiklos atkūrimo detaliajame plane (toliau – Veiklos atkūrimo detalusis planas) (1 priedas), įvyksta saugumo incidentas, dėl kurio sutrinka informacinės sistemos veiklos tęstinumas ir tampa aišku, kad atkurti informacinės sistemos veikimą per 8 val. nepavyks.

5. Už Valdymo plano įgyvendinimo organizavimą atsakingas Administracijos Ūkio tarnybos vedėjas (toliau – Ūkio tarnybos vedėjas).

6. Valdymo plane nurodytomis informacinės sistemos veiklos tęstinumo procedūromis yra siekiama šių tikslų:

6.1. paskelbus apie saugumo įvykį, sutrikdžiusį informacinės sistemos veiklą, per trumpiausią terminą atkurti pagrindinių informacinės sistemos posistemių veiklą;

6.2. sustabdyti veiklą, kuri nėra gyvybiškai svarbi, kol bus visiškai atkurtas pagrindinių informacinės sistemos posistemių veiklos tęstinumas;

6.3. sušvelninti bet kokio saugumo įvykio, nurodyto Veiklos atkūrimo detaliajame plane, poveikį, atliekant šiame plane nustatytus atsakomuosius veiksmus;

6.4. sumažinti nesusipratimų ir klaidingos informacijos kiekį, pateikiant aiškų Veiklos atkūrimo detalųjį planą ir jame įvardijant atsakingus asmenis.

7. Kiekvienas naudotojas, pastebėjęs susidariusią situaciją, kuri kelia grėsmę informacinės sistemos veiklos tęstinumui, privalo:

7.1. informuoti sistemos administratorių arba Ūkio tarnybos vedėją apie pastebėtą situaciją, keliančią grėsmę informacinės sistemos veiklos tęstinumui;

7.2. rūpintis asmeniniu saugumu, vadovautis avarijos likvidavimo procedūromis, vykdyti pagalbos tarnybų nurodymus;

7.3. teikti pagalbą kitiems naudotojams nerizikuodamas savo sveikata;

7.4. tęsti veiklą, kiek tai įmanoma susidariusios situacijos sąlygomis;

7.5. pagal kompetenciją užtikrinti informacijos saugumą ir kokybę;

7.6. vykdyti Ūkio tarnybos vedėjo, sistemos administratoriaus ir saugumo įgaliotinio nurodymus;

7.7. išsaugoti informacinės sistemos veiklai gyvybiškai svarbius duomenis, kad informacinės sistemos veiklos tęstinumas vėliau galėtų būti atkurtas.

8. Valdymo planas yra parengtas ir taikomas Rokiškio rajono savivaldybės pastatui, esančiam Respublikos g. 94, Rokiškio mieste, kuriame yra Administracijos serveriai bei saugomi ir tvarkomi Administracijos valdomos ir tvarkomos informacinės sistemos duomenys.

9. Saugumo incidento metu patirti nuostoliai finansuojami iš Rokiškio rajono savivaldybės biudžeto.

10. Kriterijai, pagal kuriuos nustatoma, kad informacinės sistemos veikla atkurta, yra:

10.1. veikia visa informacinės sistemos darbui reikalinga infrastruktūra;

10.2. naudotojams prieinamos ir be kritinių klaidų veikia visos informacinės sistemos funkcijos;

10.3. atnaujinami informacinės sistemos duomenys;

10.4. išsaugomi atnaujinti informacinės sistemos duomenys;

10.5. vyksta duomenų mainai tarp informacinės sistemos posistemių ir su kitomis informacinėmis sistemomis ir registrais;

10.6. daromos informacinės sistemos duomenų atsarginės kopijos.

II. ORGANIZACINĖS NUOSTATOS

11. Sutrikus daugiau nei vienos informacinės sistemos posistemio veiklos tęstinumui, informacinės sistemos veiklos tęstinumo atkūrimas turi būti vykdomas vadovaujantis Administracijos direktoriaus patvirtintu Rokiškio rajono savivaldybės informacinės sistemos informacinių išteklių atkūrimo prioritetų sąrašu (2 priedas).

12. Įvykus saugumo įvykiui, susijusiam su serveryje įdiegta informacinės sistemos funkcionavimą užtikrinančia programine įranga ar saugomais duomenimis:

12.1. sistemos administratorius informuoja Ūkio tarnybos vedėją, vadovaujantį informacinės sistemos veiklos atkūrimui;

12.2. sistemos administratorius informaciją apie saugumo įvykį įrašo Rokiškio rajono savivaldybės informacinės sistemos elektroninės informacijos saugumo incidentų registravimo žurnale (3 priedas) (toliau – Incidentų registravimo žurnalas);

12.3. sistemos administratorius atkuria informacinės sistemos serverio, kompiuterių tinklo

veiklą, informacinės sistemos duomenis, techninės, sisteminės ir taikomosios programinės įrangos funkcionavimą ir apie tai informuoja Ūkio tarnybos vedėją;

12.4. Ūkio tarnybos vedėjas organizuoja žalos informacinės sistemos duomenims, techninei ir programinei įrangai vertinimą, koordinuoja informacinės sistemos veiklai atkurti reikalingos techninės, sisteminės ir taikomosios programinės įrangos įsigijimo procedūras.

13. Įvykus saugumo įvykiui patalpose, kuriose yra informacinės sistemos techninė ir programinė įranga:

13.1. informacinės sistemos veiklos atkūrimui vadovauja Ūkio tarnybos vedėjas;

13.2. sistemos administratorius informaciją apie incidentą įrašo Incidentų registravimo žurnale.

14. Nesant galimybių tęsti veiklą pagrindinėse informacinės sistemos patalpose, informacinės sistemos įranga per 1 dieną laikinai perkeliama į atsargines patalpas.

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

15.1. patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų;

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

15.3. ryšių kabeliai turi būti apsaugoti nuo nesankcionuoto prisijungimo.

16. Saugumo incidento metu sunaikinta techninė, sisteminė ir taikomoji programinė įranga įsigyjama Lietuvos Respublikos viešųjų pirkimų įstatymo (Žin., 1996, Nr. 84-2000; 2006, Nr. 4-102) nustatyta tvarka, įsigijimo išlaidos padengiamos Rokiškio rajono savivaldybės biudžeto lėšomis.

III. APRAŠOMOSIOS NUOSTATOS

17. Kompiuterių tinklo fizinio ar loginio sujungimo schemas parengia ir saugo Ūkio tarnyba.

18. Atsarginės duomenų kopijos saugomos atsarginėse patalpose, naudojamose informacinės sistemos veiklai atkurti kilus saugumo incidentui. Atsarginės duomenų kopijos yra perkeliamos į saugojimo vietą kiekvieną darbo dieną.

19. Atsarginės patalpos, naudojamos informacinės sistemos veiklai atkurti kilus saugumo incidentui, yra įrengtos Respublikos g. 94, Rokiškyje.

IV. VALDYMO PLANO VEIKSMINGUMO PATIKRINIMAS

20. Siekiant užtikrinti, kad Valdymo planas būtų veiksmingas ir atitiktų esamą padėtį, jis turi būti tikrinamas ir atnaujinamas ne rečiau kaip kartą per metus. Valdymo plano veiksmingumo tikrinimą organizuoja Ūkio tarnybos vedėjas. Tikrinimo metu išanalizuojama galima nenumatyta situacija, numatomi galimi jos sprendimų būdai ir parengiama Rokiškio rajono savivaldybės informacinės sistemos rizikos įvertinimo ataskaita (4 priedas) (toliau – rizikos įvertinimo ataskaita), kurioje yra apibendrinami Valdymo plano veiksmingumo tikrinimo rezultatai, nurodomi pastebėti informacinės sistemos trūkumai ir pasiūlomos šių trūkumų šalinimo priemonės. Rizikos įvertinimo ataskaitą tvirtina Administracijos direktorius.

21. Už rizikos įvertinimo ataskaitos parengimą, pateikimą Administracijos direktoriui ir trūkumų šalinimo kontrolę atsakingas Ūkio tarnybos vedėjas.

Rokiškio rajono savivaldybės informacinės
sistemos veiklos tęstinumo
valdymo plano
1 priedas

ROKIŠKIO RAJONO SAVIVALDYBĖS INFORMACINĖS SISTEMOS VEIKLOS ATKŪRIMO DETALUSIS PLANAS

Įvykis, sukeliantis elektroninės informacijos saugos incidentą	**Atsakomieji veiksmai**	**Atsakingi vykdytojai**
1	2	3
1. Patalpų pažeidimas arba praradimas, stichinė nelaimė	1.1. Esant galimybei, išjunkite ir užrakinkite visą įrangą	Ūkio tarnyba
	1.2. Įvertinkite pažeidimus ir padarytus nuostolius	Ūkio tarnyba
	1.3. Nustatykite, ar buvo prarasti kokie nors duomenys ar įranga	Ūkio tarnyba
	1.4. Jei būtina, perkelkite veiklą į atsargines patalpas	Ūkio tarnyba
	1.5. Jei yra sudarytos įrangos tiekimo sutartys, užsakykite reikalingą įrangą	Ūkio tarnyba
	1.6. Prireikus perskirstykite, kiek tai yra įmanoma, Savivaldybės išteklius, kad būtų atkurtas prioritetinių informacinės sistemos posistemių veikimas	Ūkio tarnyba
	1.7. Jei sutarčių nėra, inicijuokite ir vykdykite įrangos pirkimą	Turto valdymo ir viešųjų pirkimų skyrius, Ūkio tarnyba
	1.8. Įsigiję įrangą, atkurkite sistemos darbingumą	Ūkio tarnyba
	1.9. Jeigu būtina, atkurkite informacinės sistemos duomenis	Ūkio tarnyba
	1.10. Patikrinkite atkurtos informacinės sistemos veikimą ir duomenų teisingumą	Ūkio tarnyba
	1.11. Nustatykite, ar buvo prarasta kokia nors įranga ar duomenys	Ūkio tarnyba
2. Pavojingos medžiagos	2.1. Nustatykite, ar buvo prarasti kokie nors duomenys ar įranga	Ūkio tarnyba
	2.2. Jei būtina, perkelkite veiklą į atsargines patalpas	Ūkio tarnyba
	2.3. Jei yra sudarytos įrangos tiekimo sutartys, užsakykite reikalingą įrangą	Ūkio tarnyba
	2.4. Prireikus perskirstykite, kiek tai yra įmanoma, Savivaldybės išteklius, kad būtų atkurtas prioritetinių informacinės sistemos posistemių veikimas	Ūkio tarnyba
	2.5. Jei sutarčių nėra, inicijuokite ir vykdykite įrangos pirkimą	Turto valdymo ir viešųjų pirkimų skyrius,

		Ūkio tarnyba
	2.6. Įsigiję įrangą, atkurkite sistemos darbingumą	Ūkio tarnyba
	2.7. Jeigu būtina, atkurkite informacinės sistemos duomenis	Ūkio tarnyba
	2.8. Patikrinkite atkurtos informacinės sistemos veikimą ir duomenų teisingumą	Ūkio tarnyba
3. Gaisras	3.1. Esant galimybei, išjunkite ir užrakinkite visą įrangą	Ūkio tarnyba
	3.2. Likvidavus gaisrą įvertinkite pažeidimus ir padarytus nuostolius	Ūkio tarnyba
	3.3. Nustatykite, ar buvo prarasti kokie nors duomenys ar įranga	Ūkio tarnyba
	3.4. Jei būtina, perkelkite veiklą į atsargines patalpas	Ūkio tarnyba
	3.5. Prireikus perskirstykite, kiek tai yra įmanoma, Savivaldybės išteklius, kad būtų atkurtas prioritetinių informacinės sistemos posistemių veikimas	Ūkio tarnyba
	3.6. Jei yra sudarytos įrangos tiekimo sutartys, užsakykite reikalingą įrangą	Ūkio tarnyba
	3.7. Jei sutarčių nėra, inicijuokite ir vykdykite įrangos pirkimą	Turto valdymo ir viešųjų pirkimų skyrius, Ūkio tarnyba
	3.8. Įsigiję įrangą, atkurkite sistemos darbingumą	Ūkio tarnyba
	3.9. Jeigu būtina, atkurkite informacinės sistemos duomenis	Ūkio tarnyba
	3.10. Patikrinkite atkurtos informacinės sistemos veikimą ir duomenų teisingumą	Ūkio tarnyba, duomenų tvarkytojai
4. Patalpų užpuolimas	4.1. Nustatykite, ar buvo prarasti kokie nors duomenys ar įranga	Ūkio tarnyba
	4.2. Perkelkite veiklą į atsargines patalpas	Ūkio tarnyba
	4.3. Prireikus perskirstykite, kiek tai yra įmanoma, Savivaldybės išteklius, kad būtų atkurtas prioritetinių informacinės sistemos posistemių veikimas	Ūkio tarnyba
	4.4. Jei yra sudarytos įrangos tiekimo sutartys, užsakykite reikalingą įrangą	Ūkio tarnyba
	4.5. Jei sutarčių nėra, inicijuokite ir vykdykite įrangos pirkimą	Turto valdymo ir viešųjų pirkimų skyrius, Ūkio tarnyba
	4.6. Įsigiję įrangą, atkurkite sistemos darbingumą	Ūkio tarnyba
	4.7. Jeigu būtina, atkurkite informacinės sistemos duomenis	Ūkio tarnyba
	4.8. Patikrinkite atkurtos informacinės sistemos veikimą ir duomenų teisingumą	Ūkio tarnyba, duomenų tvarkytojai
5. Pagrindinės	5.1. Informuokite informacinės sistemos	Ūkio tarnyba

kompiuterinės įrangos praradimas, nepakenkiant patalpų funkcionalumui	naudotojus apie veiklos sutrikimus	
	5.2. Įvertinkite nuostolius, nustatykite, kokia įranga prarasta	Ūkio tarnyba
	5.3. Prireikus perskirstykite, kiek tai yra įmanoma, Savivaldybės išteklius, kad būtų atkurtas prioritetinių informacinės sistemos posistemių veikimas	Ūkio tarnyba
	5.4. Jei yra sudarytos įrangos tiekimo sutartys, užsakykite reikalingą įrangą	Ūkio tarnyba
	5.5. Jei sutarčių nėra, inicijuokite ir vykdykite įrangos pirkimą	Turto valdymo ir viešųjų pirkimų skyrius, Ūkio tarnyba
	5.6. Įsigiję įrangą, atkurkite sistemos darbingumą	Ūkio tarnyba
6. Pagrindinių darbuotojų praradimas, nepakenkiant patalpų ir įrangos funkcionalumui	6.1. Nustatykite, kokie gyvybiškai būtini įgūdžiai prarasti	Ūkio tarnyba
	6.2. Pasitelkite iš anksto numatytus pakaitinius darbuotojus, kad pakeistumėte trūkstamą personalą	Ūkio tarnyba
	6.3. Jeigu atsiradusių spragų negalima užpildyti pasitelkus pakaitinius darbuotojus, pradėkite darbuotojų paieškos ir priėmimo į darbą procedūras	Juridinis ir personalo skyrius
7. Duomenų praradimas	7.1. Nutraukite paslaugų teikimą informacinės sistemos posistemio naudotojams	Ūkio tarnyba
	7.2. Informuokite informacinės sistemos posistemio naudotojus apie veiklos sutrikimus	Ūkio tarnyba
	7.3. Tiksliai nustatykite prarastų duomenų apimtį ir praradimo priežastis	Ūkio tarnyba
	7.4. Nustatykite, ar paskutinės atsarginės kopijos yra patikimos	Ūkio tarnyba
	7.5. Atkurkite informacinės sistemos posistemio darbingumą	Ūkio tarnyba
	7.6. Nustatykite, ar atkurti duomenys yra patikimi	Ūkio tarnyba
	7.7. Jeigu duomenys buvo prarasti dėl saugumo spragų, pašalinkite jas	Ūkio tarnyba
	7.8. Praneškite informacinės sistemos posistemio, kurios duomenų nebuvo įmanoma atkurti, naudotojams, kad duomenis reikia įvesti iš naujo	Ūkio tarnyba
	7.9. Atkurkite informacinės sistemos posistemio naudotojų galimybę naudotis sistema, kad jie galėtų iš naujo įvesti prarastus duomenis	Ūkio tarnyba
	7.10. Atkurkite informacinės sistemos posistemio duomenis iš paskutinės, žinodami, kad ji gera, atsarginės kopijos;	Ūkio tarnyba
	7.11. Atkurkite visas informacinės sistemos posistemio naudotojų galimybes naudotis informacine sistema.	Ūkio tarnyba

8. Informacinės sistemos veiklos sutrikdymas dėl kibernetinių atakų	8.1. Informuokite informacinės sistemos naudotojus apie veiklos sutrikimus	Ūkio tarnyba
	8.2. Nustatykite trikdžių šaltinį	Ūkio tarnyba
	8.3. Nustatę, jog trikdžių šaltinis yra už Savivaldybės ribų, praneškite informacinės sistemos ryšio paslaugų teikėjui apie įvykį	Ūkio tarnyba
	8.4. Nustatykite, ar neprarasti arba nesugadinti informacinės sistemos duomenys	Ūkio tarnyba
	8.5. Pašalinę trikdžius, atkurkite sistemos darbingumą	Ūkio tarnyba
	8.6. Jeigu būtina, atkurkite duomenis	Ūkio tarnyba
9. Būtinųjų komunalinių paslaugų teikimo sutrikimai	9.1. Informuokite informacinės sistemos naudotojus apie veiklos sutrikimus	Ūkio tarnyba
	9.2. Kreipkitės į komunalinių paslaugų teikėjus dėl sutrikimų pašalinimo	Ūkio tarnyba
	9.3. Organizuokite alternatyvų būtinųjų komunalinių paslaugų teikimą	Ūkio tarnyba
	9.4. Kai bus atnaujintas būtinųjų komunalinių paslaugų teikimas, atnaujinkite informacinės sistemos veikimą	Ūkio tarnyba
10. Ryšio sutrikimai	10.1. Informuokite informacinės sistemos naudotojus apie veiklos sutrikimus	Ūkio tarnyba
	10.2. Nustatykite ryšio paslaugų teikimo sutrikimo priežastis	Ūkio tarnyba
	10.3. Kreipkitės į ryšio paslaugų teikėjus dėl sutrikimų pašalinimo	Ūkio tarnyba
	10.4. Organizuokite alternatyvų gyvybiškai svarbių ryšio paslaugų teikimą	Ūkio tarnyba

---

Rokiškio rajono savivaldybės informacinės
sistemos veiklos tęstinumo
valdymo plano
2 priedas

(Rokiškio rajono savivaldybės informacinės sistemos informacinių išteklių atkūrimo prioritetų sąrašo forma)

TVIRTINU
Direktorius

ROKIŠKIO RAJONO SAVIVALDYBĖS INFORMACINĖS SISTEMOS INFORMACINIŲ IŠTEKLIŲ ATKŪRIMO PRIORITETAI

_____ Nr. _____

Prioritetas	**Informacinės sistemos posistemio pavadinimas**

_____

Rokiškio rajono savivaldybės informacinės
sistemos veiklos tęstinumo
valdymo plano
3 priedas

(Rokiškio rajono savivaldybės informacinės sistemos elektroninės informacijos saugos incidentų registravimo žurnalo forma)

ROKIŠKIO RAJONO SAVIVALDYBĖS INFORMACINĖS SISTEMOS ELEKTRONINĖS INFORMACIJOS SAUGUMO INCIDENTŲ REGISTRAVIMO ŽURNALAS

Pildymo pradžia
20__ m. _____ d.

Eil. Nr.	Elektroninės informacijos saugumo incidentas					
	Pranešimą pateikęs darbuotojas/padalinys	Požymio kodas	Įvykio aprašymas	Pradžia (metai, mėnuo, diena, valanda)	Pabaiga (metai, mėnuo, diena, valanda)	Pastabos

Elektroninės informacijos saugumo incidentų požymių kodai:

1 – patalpų pažeidimas arba praradimas, stichinė nelaimė.
2 – pavojingos medžiagos.
3 – gaisras.
4 – patalpų užpuolimas.
5 – pagrindinės kompiuterinės įrangos praradimas, nepakenkiant patalpų funkcionalumui.
6 – pagrindinių darbuotojų praradimas, nepakenkiant patalpų ir įrangos funkcionalumui.
7 – duomenų praradimas.
8 – informacinės sistemos veiklos sutrikdymas dėl kibernetinių atakų.
9 – būtinųjų komunalinių paslaugų teikimo sutrikimai.
10 – ryšio sutrikimai.

_____

Rokiškio rajono savivaldybės informacinės
sistemos veiklos tęstinumo
valdymo plano
4 priedas

(Rizikos įvertinimo ataskaitos forma)

TVIRTINU
Direktorius

ROKIŠKIO RAJONO SAVIVALDYBĖS INFORMACINĖS SISTEMOS RIZIKOS ĮVERTINIMO ATASKAITA

_____ Nr. _____

Rizikos veiksniai	**Trūkumai**	**Prevencinės priemonės rizikos veiksniams išvengti**		
		apibūdinimas	**vykdymo terminas**	**atsakingas vykdytojas**
1. Patalpų pažeidimas arba praradimas, stichinė nelaimė				
2. Pavojingos medžiagos				
3. Gaisras				
4. Patalpų užpuolimas				
5. Pagrindinės kompiuterinės įrangos praradimas, nepakenkiant patalpų funkcionalumui				
6. Pagrindinių darbuotojų praradimas, nepakenkiant patalpų ir įrangos funkcionalumui				
7. Duomenų praradimas				
8. Informacinės sistemos veiklos sutrikdymas dėl kibernetinių atakų				
9. Būtinųjų komunalinių paslaugų teikimo sutrikimai				
10. Ryšio sutrikimai				

(pareigos) (parašas) (vardas, pavardė)

_____

PATVIRTINTA
Rokiškio rajono savivaldybės administracijos
direktoriaus 2015 m. gruodžio 23 d.
įsakymu Nr. AV-1090

ROKIŠKIO RAJONO SAVIVALDYBĖS KOMPIUTERIZUOTOS INFORMACINĖS SISTEMOS VARTOTOJO INSTRUKCIJA

1. Rokiškio rajono savivaldybės kompiuterizuotos informacinės sistemos (toliau – KIS) vartotojo instrukcija reglamentuoja darbą KIS sistemoje.

2. Naujai įregistruotas KIS vartotojas gauna:

2.1. vartotojo identifikavimo kodą (toliau – IK) ir pradinį slaptažodį, skirtus prisijungti prie sistemos;

2.2. prieigą prie Savivaldybės administracijos dokumentų;

2.3. elektroninio pašto dėžutę KIS pašto.

3. KIS vartotojas privalo:

3.1. pasikeisti pradinį slaptažodį pirmojo prisijungimo prie sistemos metu;

3.2. prisijungdamas prie sistemos naudoti tik savo IK ir slaptažodį. Jei kyla abejonių dėl slaptažodžio slaptumo, vartotojas dėl jo pakeitimo privalo kreiptis į Ūkio tarnybą;

3.3. prieš palikdamas kompiuterizuotą darbo vietą, užbaigti darbą kaip KIS vartotojas (atsijungti nuo sistemos arba „užrakinti“ (*lock computer*) priėjimą prie darbo vietos);

3.4. naudotis internetu bei kitais jam suteiktais KIS ištekliais tik savo tiesioginiam darbui atlikti;

3.5. darbo vietoje naudotis tik KIS elektroninio pašto dėžute;

4. KIS vartotojui draudžiama:

4.1. leisti naudotis savo IK ir slaptažodžiu kitiems asmenims;

4.2. laikyti serveryje garso, vaizdo ir kitas bylas, nesusijusias su tiesioginiu darbu.

5. KIS vartotojui, naudojančiam Savivaldybės administracijos suteiktą kompiuterinę techniką, draudžiama:

5.1. keisti nustatytą programinių priemonių konfigūraciją;

5.2. pakeisti, papildyti ar ištrinti naudojamą programinę įrangą;

5.3. įdiegti programinę įrangą;

5.4. naudoti iš informacinių laikmenų perrašytą ar kompiuterių tinklais iš interneto ar kitų šaltinių atsiųstą programinę įrangą;

5.5. pakeisti nustatytą kompiuterinės technikos komplektą ir ardyti kompiuterinę techniką;

5.6. siųstis internetu, elektroniniu paštu bei kitais būdais garso, vaizdo ir kitas bylas, nesusijusias su tiesioginiu darbu.

Susipažinau

(pareigos) (parašas) (vardas ir pavardė)

(data)