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

ROKIŠKIO RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS

I. BENDROSIOS NUOSTATOS

1. Rokiškio rajono savivaldybės administracijos (toliau – Administracija) informacinės sistemos (toliau – informacinė sistema) veiklos tęstinumo valdymo plano (toliau – Valdymo planas) tikslas – nustatyti Savivaldybės administracijos 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 veiklos tęstinumo valdymo grupė (toliau – valdymo grupė) – įstaigos vadovo įsakymu sudaryta asmenų grupė, kuri atlieka situacijos analizę ir priima sprendimus informacinės sistemos veiklos tęstinumo valdymo klausimais bei koordinuoja jų įgyvendinimą.

Informacinės sistemos veiklos atkūrimo grupė (toliau – atkūrimo grupė) – tarnybinių stočių, kompiuterių tinklo, taikomųjų programų ir kt. veiklą atkuriantys asmenys.

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 adminsitracijos 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 direktorius.

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, saugumo įgaliotinį arba Komunikacijos ir kultūros skyriaus 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 Komunikacijos ir kultūros skyriaus vedėjo, saugumo įgaliotinio, sistemos administratoriaus 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 Sąjūdžio g. 1, Rokiškio mieste, kuriame yra Administracijos serveriai bei saugomi ir tvarkomi Administracijos valdomos ir tvarkomos informacinės sistemos duomenys.

8.1 Valdymo plane numatytų veiksmų privalo laikytis informacinės sistemos tvarkytojai, valdytojai, saugos įgaliotinis, administratorius ir informacinės sistemos naudotojai.

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. Elektroninės informacijos saugos incidentams valdyti ir veiklos atkūrimui organizuoti Administracijos direktoriaus įsakymu tvirtinamos 2 grupės: Informacinės sistemos veiklos tęstinumo valdymo grupė ir Veiklos atkūrimo grupė.

12. Valdymo grupę sudaro:

12.1. Valdymo grupės vadovas – Rokiškio rajono savivaldybės administracijos direktorius (toliau – Administracijos direktorius);

12.2. Valdymo grupės vadovo pavaduotojas – Komunikacijos ir kultūros skyriaus vedėjas;

12.3. Valdymo grupės nariai: saugumo įgaliotinis; Bendrojo skyriaus vedėjas; Finansų skyriaus vedėjas; Centralizuotos buhalterinės apskaitos skyriaus vedėjas; Socialinės apsaugos ir sveikatos skyriaus vedėjo pavaduotojas, vyresnysis specialistas civilinei saugai ir mobilizacijai, duomenų apsaugos pareigūnas.

13. Valdymo grupės funkcijos, užtikrinant veiklos tęstinumą:

13.1. situacijos analizė ir sprendimų informacinės sistemos veiklos tęstinumo valdymo klausimais priėmimas;

13.2. bendravimas su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;

13.3. bendravimas su susijusių informacinių sistemų veiklos tęstinumo valdymo grupėmis;

bendravimas su teisėsaugos ir kitomis institucijomis, institucijos darbuotojais ir kitomis interesų grupėmis;

13.4. finansinių ir kitų išteklių, reikalingų informacinės sistemos veiklai atkurti, įvykus elektroninės informacijos saugos incidentui, naudojimo kontrolė;

13.5. elektroninės informacijos fizinė sauga įvykus elektroninės informacijos saugos incidentui;

13.6. logistika (žmonių, daiktų, įrangos gabenimas ir jo organizavimas);

13.7. informacinės sistemos veiklos atkūrimo priežiūra ir koordinavimas;

13.8. kitos veiklos tęstinumo valdymo grupei pavestos funkcijos;

14. Veiklos atkūrimo grupę sudaro:

14.1. Veiklos atkūrimo grupės vadovas – Komunikacijos ir kultūros skyriaus vedėjas;

14.2. Veiklos atkūrimo grupės vadovo pavaduotojas – saugumo įgaliotinis;

14.3. Veiklos atkūrimo grupės nariai – sistemos administratoriai.

15. Atkūrimo grupės funkcijos:

15.1. tarnybinių stočių veikimo atkūrimo organizavimas;

15.2. kompiuterių tinklo veikimo atkūrimo organizavimas;

15.3. informacinės sistemos elektroninės informacijos atkūrimo organizavimas;

15.4. taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

15.5. darbo kompiuterių veikimo atkūrimo ir prijungimo prie kompiuterių tinklo organizavimas;

15.6. kitos atkūrimo grupei pavestos funkcijos;

16. 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 (3 priedas).

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

17.1. sistemos administratorius informuoja saugumo įgaliotinį, vadovaujantį informacinės sistemos veiklos atkūrimui;

17.2. sistemos administratorius informaciją apie saugumo įvykį įrašo Rokiškio rajono savivaldybės administracijos informacinės sistemos elektroninės informacijos saugumo incidentų registravimo žurnale (4 priedas) (toliau – Incidentų registravimo žurnalas);

17.3. sistemos administratorius atkuria informacinės sistemos serverio, kompiuterių tinklo veiklą, informacinės sistemos duomenis, techninės, sisteminės ir taikomosios programinės įrangos funkcionavimą ir apie tai informuoja saugumo įgaliotinį ir Komunikacijos ir kultūros skyriaus vedėją;

17.4. saugumo įgaliotinis organizuoja žalos informacinės sistemos duomenims, techninei ir programinei įrangai vertinimą, koordinuoja informacinės sistemos veiklai atkurti reikalingos

techninės, sisteminės ir taikomosios programinės įrangos įsigijimo procedūras.

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

18.1. informacinės sistemos veiklos atkūrimui vadovauja saugumo įgaliotinis;

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

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

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

20.1. patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų;

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

20.3. ryšių kabeliai turi būti apsaugoti nuo nesankcionuoto prisijungimo.

21. Įvykus kibernetinio saugumo incidentui, vadovaujamasi informacinės sistemos kibernetinių incidentų valdymo planu (2 priedas), kurio veiksmai suskirstyti į du etapus:

21.1. Kibernetinio incidento įvertinimas, ir priskyrimas, priemonių pavojui sustabdyti ir padarytai žalai likviduoti sudarymas;

21.2. Kibernetinio incidento pasekmes likviduojančių darbuotojų paskyrimas pasekmes likviduojančių darbuotojų instruktavimas, jų veiksmų koordinavimas. Kibernetinio incidento pašalinimas.

22. Saugumo incidento metu sunaikinta techninė, sisteminė ir taikomoji programinė įranga įsigyjama Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka, įsigijimo išlaidos padengiamos Rokiškio rajono savivaldybės biudžeto lėšomis.

23. Esant incidentui, Valdymo ir Atkūrimo grupės organizuoja pasitarimus, atsižvelgdamos į Valdymo grupės pirmojo susitikimo metu nustatytą dažnumą, palaiko ryšius visomis tuo metu prieinamomis priemonėmis (el. paštu, mobiliuoju ryšiu ir kt.). Valdymo grupė ir Atkūrimo grupė turi teisę kviesti į pasitarimus informacinių sistemų tvarkytojų atstovus.

III. APRAŠOMOSIOS NUOSTATOS

24. Komunikacijos ir kultūros skyrius saugo:

24.1. kompiuterių tinklo fizinio ar loginio sujungimo schemas;

24.2. specifikaciją, kurioje nurodomas Informacinių sistemų administratorius pavaduojančių asmenų minimalus kompetencijos ar žinių lygis;

24.3 specifikaciją, kurioje nurodomas minimalaus funkcionalumo informacinių technologijų įrangos, tinkamos institucijos poreikius atitinkančiai informacinės sistemos veiklai užtikrinti įvykus elektroninės informacijos saugos incidentui;

24.4. dokumentą, kuriame nurodytos elektroninės informacijos teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutartys, atsakingų už šių sutarčių įgyvendinimo priežiūrą asmenų pareigos;

24.5. dokumentą, kuriame nurodyta programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos;

24.6. dokumentą, kuriame nurodytas veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės narių sąrašas su kontaktiniais duomenimis, leidžiančiais pasiekti šiuos asmenis bet kuriuo metu.

25.Turto valdymo ir ūkio skyrius saugo:

25.1. dokumentas, kuriame nurodyti kiekvieno pastato, kuriame yra informacinės sistemos įranga, aukšto patalpų brėžiniai ir juose pažymėti:

25.1.1 tarnybinės stotys;

25.1.2. kompiuterių tinklo ir telefonų tinklo mazgai;

25.1.3. kompiuterių tinklo ir telefonų tinklo laidų vedimo tarp pastato aukštų vietos;
25.1.4 elektros įvedimo pastate vietos;

26. 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.

27. Atsarginės patalpos, naudojamos informacinės sistemos veiklai atkurti kilus saugumo incidentui, yra įrengtos Sąjūdžio a. 1, Rokiškyje.

IV. VALDYMO PLANO VEIKSMINGUMO PATIKRINIMAS

27. Saugumo įgaliotinis organizuoja Administracijos darbuotojų supažindinimą su šiuo planu.

28. Plano veiksmingumas turi būti išbandomas kartą per metus. Valdymo plano veiksmingumo tikrinimą organizuoja saugumo įgaliotinis kartu su sistemos administratoriais. Tikrinimo metu išanalizuojama galima nenumatyta situacija, numatomi galimi jos sprendimų būdai ir parengiama Rokiškio rajono savivaldybės administracijos informacinės sistemos rizikos įvertinimo ataskaita (5 priedas) (toliau – rizikos įvertinimo ataskaita), kurioje yra apibendrinami Valdymo plano veiksmingumo tikrinimo rezultatai, nurodomi pastebėti informacinės sistemos trūkumai ir pasiūlomos šių trūkumų šalinimo priemonės.

29. Saugumo įgaliotinis organizuoja plano veiksmingumo išbandymo metu pastebėtų trūkumų ataskaitos parengimą ir pateikimą Administracijos direktoriui ir ne vėliau kaip per penkias darbo dienas kopijos pateikimą Nacionaliniam kibernetinio saugumo centrui, taip pat plano atnaujinimą po plano veiksmingumo bandymų ir (arba) rizikos veiksnių įvertinimo.

30. Plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami remiantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

Rokiškio rajono savivaldybės administracijos informacinės sistemos veiklos tęstinumo valdymo plano
1 priedas

ROKIŠKIO RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINĖS SISTEMOS VEIKLOS ATKŪRIMO DETALUSIS PLANAS

Įvykis, sukeliantis elektroninės informacijos saugos incidentą	**Atsakomieji veiksmai**	**Atsakingi vykdytojai**	**Terminai**
1	2	3	4
	1.1. Esant galimybei, išjunkite ir užrakinkite visą įrangą	Veiklos atkūrimo grupė	Nedelsiant
	1.2. Įvertinkite pažeidimus ir padarytus nuostolius	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento

1. Patalpų pažeidimas arba praradimas, stichinė nelaimė			nustatymo
	1.3. Nustatykite, ar buvo prarasti kokie nors duomenys ar įranga	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
	1.4. Jei būtina, perkelkite veiklą į atsargines patalpas	Veiklos atkūrimo grupė	Per vieną darbo dieną po incidento nustatymo
	1.5. Jei yra sudarytos įrangos tiekimo sutartys, užsakykite reikalingą įrangą	Veiklos atkūrimo grupė	Per teisės aktuose numatytą terminą
	1.6. Prireikus perskirstykite, kiek tai yra įmanoma, Savivaldybės išteklius, kad būtų atkurtas prioritetinių informacinės sistemos posistemių veikimas	Veiklos atkūrimo grupė	Per dvi darbo dienas po incidento likvidavimo
	1.7. Jei sutarčių nėra, inicijuokite ir vykdykite įrangos pirkimą	Veiklos atkūrimo grupė	Per teisės aktuose numatytą terminą
	1.8. Įsigiję įrangą, atkurkite sistemos darbingumą	Veiklos atkūrimo grupė	Per vieną darbo dieną po įrangos įsigijimo
	1.9. Jeigu būtina, atkurkite informacinės sistemos duomenis	Veiklos atkūrimo grupė	Per vieną darbo dieną po papildomų išteklių įsigijimo
	1.10. Patikrinkite atkurtos informacinės sistemos veikimą ir duomenų teisingumą	Veiklos atkūrimo grupė	Per dvi valandas po sistemos atkūrimo proceso
	1.11. Nustatykite, ar buvo prarasta kokia nors įranga ar duomenys	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
2. Pavojingos medžiagos	2.1. Nustatykite, ar buvo prarasti kokie nors duomenys ar įranga	Veiklos atkūrimo grupė	Per vieną darbo dieną po incidento nustatymo
	2.2. Jei būtina, perkelkite veiklą į atsargines patalpas	Veiklos atkūrimo grupė	Per penkiolika darbo valandų nuo incidento nustatymo
	2.3. Jei yra sudarytos įrangos tiekimo sutartys, užsakykite reikalingą įrangą	Veiklos atkūrimo grupė	Per teisės aktuose numatytą terminą

	2.4. Prireikus perskirstykite, kiek tai yra įmanoma, Savivaldybės išteklius, kad būtų atkurtas prioritetinių informacinės sistemos posistemių veikimas	Veiklos atkūrimo grupė	Per dvi darbo dienas po incidento likvidavimo
	2.5. Jei sutarčių nėra, inicijuokite ir vykdykite įrangos pirkimą	Veiklos atkūrimo grupė	Per teisės aktuose numatytą terminą
	2.6. Įsigiję įrangą, atkurkite sistemos darbingumą	Veiklos atkūrimo grupė	Per vieną darbo dieną po įrangos įsigijimo
	2.7. Jeigu būtina, atkurkite informacinės sistemos duomenis	Veiklos atkūrimo grupė	Per tris darbo valandas po sistemos darbingumo atkūrimo
	2.8. Patikrinkite atkurtos informacinės sistemos veikimą ir duomenų teisingumą	Veiklos atkūrimo grupė	Per dvi darbo valandas po atkurtų informacinės sistemos duomenų
3. Gaisras	3.1. Esant galimybei, išjunkite ir užrakinkite visą įrangą	Veiklos atkūrimo grupė	Nedelsiant
	3.2. Likvidavus gaisrą įvertinkite pažeidimus ir padarytus nuostolius	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
	3.3. Nustatykite, ar buvo prarasti kokie nors duomenys ar įranga	Veiklos atkūrimo grupė	Per vieną darbo valandą
	3.4. Jei būtina, perkelkite veiklą į atsargines patalpas	Veiklos atkūrimo grupė	Per penkias darbo dienas po incidento likvidavimo
	3.5. Prireikus perskirstykite, kiek tai yra įmanoma, Savivaldybės išteklius, kad būtų atkurtas prioritetinių informacinės sistemos posistemių veikimas	Veiklos atkūrimo grupė	Per dvi darbo dienas po incidento likvidavimo
	3.6. Jei yra sudarytos įrangos tiekimo sutartys, užsakykite reikalingą įrangą	Veiklos atkūrimo grupė	Per teisės aktuose numatytą terminą
	3.7. Jei sutarčių nėra, inicijuokite ir vykdykite įrangos pirkimą	Veiklos atkūrimo grupė	Per teisės aktuose numatytą terminą
	3.8. Įsigiję įrangą, atkurkite sistemos darbingumą	Veiklos atkūrimo grupė	Per vieną darbo dieną po įrangos

			įsigijimo
	3.9. Jeigu būtina, atkurkite informacinės sistemos duomenis	Veiklos atkūrimo grupė	Per vieną darbo dieną po įrangos įsigijimo
	3.10. Patikrinkite atkurtos informacinės sistemos veikimą ir duomenų teisingumą	Veiklos atkūrimo grupė	Per penkias valandas po informacinės sistemos atkūrimo
4. Patalpų užpuolimas	4.1. Nustatykite, ar buvo prarasti kokie nors duomenys ar įranga	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
	4.2. Perkelkite veiklą į atsargines patalpas	Veiklos atkūrimo grupė	Per vieną darbo dieną po incidento nustatymo
	4.3. Prireikus perskirstykite, kiek tai yra įmanoma, Savivaldybės išteklius, kad būtų atkurtas prioritetinių informacinės sistemos posistemių veikimas	Veiklos atkūrimo grupė	Per dvi darbo dienas po incidento likvidavimo
	4.4. Jei yra sudarytos įrangos tiekimo sutartys, užsakykite reikalingą įrangą	Veiklos atkūrimo grupė	Per teisės aktuose numatytą terminą
	4.5. Jei sutarčių nėra, inicijuokite ir vykdykite įrangos pirkimą	Veiklos atkūrimo grupė	Per teisės aktuose numatytą terminą
	4.6. Įsigiję įrangą, atkurkite sistemos darbingumą	Veiklos atkūrimo grupė	Per vieną darbo dieną po įrangos įsigijimo
	4.7. Jeigu būtina, atkurkite informacinės sistemos duomenis	Veiklos atkūrimo grupė	Per vieną darbo dieną po įrangos įsigijimo
	4.8. Patikrinkite atkurtos informacinės sistemos veikimą ir duomenų teisingumą	Veiklos atkūrimo grupė	Per penkias valandas
5. Pagrindinės kompiuterinės įrangos praradimas, nepakenkiant patalpų funkcionalumui	5.1. Informuokite informacinės sistemos naudotojus apie veiklos sutrikimus	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
	5.2. Įvertinkite nuostolius, nustatykite, kokia įranga prarasta	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
	5.3. Prireikus perskirstykite, kiek tai yra įmanoma, Savivaldybės išteklius,	Veiklos atkūrimo grupė	Per dvi darbo dienas po

	kad būtų atkurtas prioritetinių informacinės sistemos posistemių veikimas		incidento likvidavimo
	5.4. Jei yra sudarytos įrangos tiekimo sutartys, užsakykite reikalingą įrangą	Veiklos atkūrimo grupė	Per teisės aktuose nustatytą terminą
	5.5. Jei sutarčių nėra, inicijuokite ir vykdykite įrangos pirkimą	Veiklos atkūrimo grupė	Per teisės aktuose numatytą terminą
	5.6. Įsigiję įrangą, atkurkite sistemos darbingumą	Veiklos atkūrimo grupė	Per vieną darbo dieną po įrangos įsigijimo
6. Pagrindinių darbuotojų praradimas, nepakenkiant patalpų ir įrangos funkcionalumui	6.1. Nustatykite, kokie gyvybiškai būtini įgūdžiai prarasti	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
	6.2. Pasitelkite iš anksto numatytus pakaitinius darbuotojus, kad pakeistumėte trūkstamą personalą	Veiklos atkūrimo grupė	Per teisės aktuose numatytą terminą
	6.3. Jeigu atsiradusių spragų negalima užpildyti pasitelkus pakaitinius darbuotojus, pradėkite darbuotojų paieškos ir priėmimo į darbą procedūras	Juridinis ir personalo skyrius	Per teisės aktuose numatytą terminą
7. Duomenų praradimas	7.1. Nutraukite paslaugų teikimą informacinės sistemos posistemio naudotojams	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
	7.2. Informuokite informacinės sistemos posistemio naudotojus apie veiklos sutrikimus	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
	7.3. Tiksliai nustatykite prarastų duomenų apimtį ir praradimo priežastis	Veiklos atkūrimo grupė	Per vieną darbo dieną
	7.4. Nustatykite, ar paskutinės atsarginės kopijos yra patikimos	Veiklos atkūrimo grupė	Per dvi darbo valandas po prarastų duomenų atstatymo
	7.5. Atkurkite informacinės sistemos posistemio darbingumą	Veiklos atkūrimo grupė	Per dvi darbo valandas
	7.6. Nustatykite, ar atkurti duomenys yra patikimi	Veiklos atkūrimo grupė	Per dvi darbo valandas
	7.7. Jeigu duomenys buvo prarasti dėl saugumo spragų, pašalinkite jas	Veiklos atkūrimo grupė	Per vieną darbo dieną
	7.8. Praneškite informacinės sistemos posistemio, kurios duomenų nebuvo	Veiklos atkūrimo grupė	Per vieną darbo valandą

	įmanoma atkurti, naudotojams, kad duomenis reikia įvesti iš naujo		po prarastų duomenų atstatymo
	7.9. Atkurkite informacinės sistemos posistemio naudotojų galimybę naudotis sistema, kad jie galėtų iš naujo įvesti prarastus duomenis	Veiklos atkūrimo grupė	Per vieną darbo dieną po prarastų duomenų atstatymo ir įvertinimo
	7.10. Atkurkite informacinės sistemos posistemio duomenis iš paskutinės, žinodami, kad ji gera, atsarginės kopijos;	Veiklos atkūrimo grupė	Per vieną darbo dieną
	7.11. Atkurkite visas informacinės sistemos posistemio naudotojų galimybes naudotis informacine sistema.	Veiklos atkūrimo grupė	Per tris darbo dienas
8. Informacinės sistemos veiklos sutrikdymas dėl kibernetinių atakų	8.1. Informuokite informacinės sistemos naudotojus apie veiklos sutrikimus	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
	8.2. Nustatykite trikdžių šaltinį	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
	8.3. Nustatę, jog trikdžių šaltinis yra už Savivaldybės ribų, praneškite informacinės sistemos ryšio paslaugų teikėjui apie įvykį	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
	8.4. Nustatykite, ar neprarasti arba nesugadinti informacinės sistemos duomenys	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
	8.5. Pašalinę trikdžius, atkurkite sistemos darbingumą	Veiklos atkūrimo grupė	Per tris darbo dienas
	8.6. Jeigu būtina, atkurkite duomenis	Veiklos atkūrimo grupė	Per penkias darbo dienas
9. Būtinųjų komunalinių paslaugų teikimo sutrikimai	9.1. Informuokite informacinės sistemos naudotojus apie veiklos sutrikimus	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
	9.2. Kreipkitės į komunalinių paslaugų teikėjus dėl sutrikimų pašalinimo	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
	9.3. Organizuokite alternatyvų būtinųjų komunalinių paslaugų teikimą	Veiklos atkūrimo grupė	Per tris darbo dienas
	9.4. Kai bus atnaujintas būtinųjų komunalinių paslaugų teikimas, atnaujinkite informacinės sistemos veikimą	Veiklos atkūrimo grupė	Per vieną darbo dieną po komunalinių paslaugų

			teikimo atstatymo
10. Ryšio sutrikimai	10.1. Informuokite informacinės sistemos naudotojus apie veiklos sutrikimus	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
	10.2. Nustatykite ryšio paslaugų teikimo sutrikimo priežastis	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
	10.3. Kreipkitės į ryšio paslaugų teikėjus dėl sutrikimų pašalinimo	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
	10.4. Organizuokite alternatyvų gyvybiškai svarbių ryšio paslaugų teikimą	Veiklos atkūrimo grupė	Per dvi darbo dienas

Rokiškio rajono savivaldybės administracijos informacinės sistemos veiklos tęstinumo valdymo plano
2 priedas

ROKIŠKIO RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINĖS SISTEMOS KIBERNETINIŲ INCIDENTŲ VALDYMO PLANAS

Etapai	Veiksmai	Atsakingi vykdytojai
1. Kibernetinio incidento įvertinimas, ir priskyrimas, priemonių pavojui sustabdyti ir padarytai žalai likviduoti sudarymas	1.1. Kibernetinio incidento nustatymas (gavus informaciją iš kibernetinio saugumo priemonių, Naudotojų, Administratoriaus, kibernetinius incidentus valdančių ir (ar) tiriančių institucijų, kitų juridinių asmenų ar kitų valstybių arba tarptautinių organizacijų ar institucijų, atliekančių kibernetinio saugumo užtikrinimo funkcijas). Nenustačius kibernetinio incidento požymių, ne vėliau kaip per 4 valandas informuojamos kibernetinius incidentus valdančios ir (ar) tiriančios institucijos, jei jos pateikė informaciją apie galimą kibernetinį incidentą.	Saugumo įgaliotinis
	1.2. Kibernetinio incidento įvertinimas ir užregistravimas.	Saugumo įgaliotinis
	1.3. Pranešti Nacionaliniam kibernetinio saugumo centrui naudojantis Kibernetinio saugumo informaciniu tinklu, o nesant galimybės Nacionalinio kibernetinio saugumo centro nurodytais kontaktais apie: • didelės reikšmės kibernetinį incidentą – nedelsiant, bet ne vėliau kaip per vieną valandą nuo jų nustatymo; • vidutinės reikšmės kibernetinį incidentą – ne vėliau kaip per keturias valandas nuo jų nustatymo; • nereikšmingą kibernetinį incidentą – periodiškai kiekvieno kalendorinio mėnesio pirmą darbo dieną teikiant apibendrintą informaciją apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo teikimo dienos, skaičių. Pranešime Nacionaliniam kibernetinio saugumo centrui nurodoma: • kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal Plano 4 priede pateiktus kriterijus; • trumpas kibernetinio incidento apibūdinimas; • tikslus laikas, kada kibernetinis incidentas	Saugumo įgaliotinis

	įvyko ir buvo nustatytas; • kibernetinio incidento šalinimo tvarka (nurodant, ar tai prioritetas, ar ne); • tikslus laikas, kada bus teikiama kibernetinio incidento tyrimo ataskaita.	
	1.4. Informacijos apie kibernetinius saugos incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių saugos incidentų valdymo priemones pateikimas Valstybinei duomenų apsaugos inspekcijai šios institucijos nustatyta tvarka ir sąlygomis	Saugumo įgaliotinis, Duomenų apsaugos pareigūnas
	1.5. Informacijos, reikalingos kibernetiniams saugos incidentams, turintiems nusikalstamos veikos požymių, užkardyti ir tirti, pateikimas policijai. Informacija pateikiama policijos generalinio komisaro nustatyta tvarka ir sąlygomis	Saugumo įgaliotinis
	1.6. Kibernetinio incidento įrodymų surinkimas	Administratoriai
	1.7. Kibernetinio incidento tyrimas	Saugumo įgaliotinis
	1.8. Priemonių sustabdyti ir padarytai žalai likviduoti sudarymas	Veiklos atkūrimo grupės vadovas
2. Kibernetinio incidento pasekmes likviduojančių darbuotojų paskyrimas Pasekmes likviduojančių darbuotojų instruktavimas, jų veiksmų koordinavimas. Kibernetinio incidento pašalinimas.	2.1. Kibernetinio incidento pasekmes likviduojančių darbuotojų paskyrimas	Veiklos atkūrimo grupės vadovas
	2.2. Pasekmes likviduojančių darbuotojų instruktavimas, jų veiksmų koordinavimas	Saugumo įgaliotinis
	2.3. Kibernetinio incidento šalinimas	Administratoriai
	2.4. Parengti kibernetinio incidento tyrimo ataskaitą, kurioje nurodoma: • ryšių ir informacinės sistemos, kurioje nustatytas kibernetinis incidentas, tipas (elektroninių ryšių tinklas, informacinė sistema, registras, pramoninių procesų valdymo sistema, tarnybinė stotis ir panašiai); • kibernetinio incidento veikimo trukmė; • kibernetinio incidento šaltinis; • kibernetinio incidento požymiai; • kibernetinio incidento veikimo metodas; • galimos ir (ar) nustatytos kibernetinio incidento pasekmės; • kibernetinio incidento poveikio pasireiškimo (galimo išplitimo) mastas; • kibernetinio incidento būsena (aktyvus, pasyvus); • priemonės, kuriomis kibernetinis incidentas nustatytas; • galimos ir (ar) taikomos kibernetinio incidento valdymo priemonės; • tikslus laikas, kada bus teikiama pakartotinė	Saugumo įgaliotinis

	kibernetinio incidento tyrimo ataskaita, jei Kibernetinis incidentas nepašalintas.	
	2.5. Nacionaliniam kibernetinio saugumo centrui naudojantis Kibernetinio saugumo informaciniu tinklu, o nesant galimybės Nacionalinio kibernetinio saugumo centro nurodytais kontaktais, pateikti kibernetinio incidento tyrimo ataskaitą: • 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; • 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	Saugumo įgaliotinis
	2.6. Įvertinti, ar kibernetinį incidentą pavyks suvaldyti patiems. Jei ne, prašoma Nacionalinio kibernetinio saugumo centro pagalbos ir vykdomi jų nurodymai	Veiklos atkūrimo grupės vadovas
	2.7. Kibernetinio incidento sustabdymas ir pasekmių pašalinimas	Veiklos atkūrimo grupės vadovas
	2.8. Galutinės kibernetinio tyrimo ataskaitos parengimas (patikslinimas)	Saugumo įgaliotinis
	2.9. Nacionaliniam kibernetinio saugumo centrui naudojantis Kibernetinio saugumo informaciniu tinklu, o nesant galimybės Nacionalinio kibernetinio saugumo centro nurodytais kontaktais, pateikti galutinę kibernetinio incidento tyrimo ataskaitą – didelio ar vidutinio poveikio kibernetinių incidentų suvaldymą ar pasibaigimą – ne vėliau kaip per keturias valandas nuo jų suvaldymo ar pasibaigimo	Saugumo įgaliotinis
	2.10. Informuoti Informacinės sistemos teikiamų paslaugų gavėjus, jeigu kibernetinio incidento poveikis padarė arba gali ateityje padaryti žalos ryšių ir informacinės sistemos teikiamų paslaugų gavėjui – ne vėliau kaip per aštuonias valandas nuo kibernetinio incidento suvaldymo ar pasibaigimo	Saugumo įgaliotinis
	2.11. Nustatyti kibernetinio saugumo organizacines ir technines priemones, kad kibernetinis incidentas nepasikartotų ar poveikis būtų minimalus.	Veiklos atkūrimo grupės vadovas
	2.12. Numatyti nustatytų kibernetinio saugumo organizacines ir technines priemonių įgyvendinimo terminus ir atsakingus asmenis	Veiklos valdymo grupės vadovas

Rokiškio rajono savivaldybės administracijos informacinės sistemos veiklos tęstinumo valdymo plano
3 priedas

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

TVIRTINU
Direktorius

ROKIŠKIO RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINĖS SISTEMOS INFORMACINIŲ IŠTEKLIŲ ATKŪRIMO PRIORITETAI

_____ Nr. _____

Prioritetas	**Informacinės sistemos posistemio pavadinimas**

_____

Rokiškio rajono savivaldybės administracijos informacinės sistemos veiklos tęstinumo valdymo plano
4 priedas

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

ROKIŠKIO RAJONO SAVIVALDYBĖS ADMINISTRACIJOS 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 administracijos informacinės sistemos veiklos tęstinumo valdymo plano
5 priedas

(Rizikos įvertinimo ataskaitos forma)

TVIRTINU
Direktorius

ROKIŠKIO RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINĖS SISTEMOS RIZIKOS ĮVERTINIMO ATASKAITA

_____ Nr. _____

_____ Nr. _____

Plano išbandymas (pratybos) vyko:

_____

Plano išbandyme dalyvavo Veiklos tęstinumo valdymo grupės nariai:
1. _____
2. _____
3. _____

Plano išbandymo scenarijus:

_____
_____
_____

Plano išbandymo eiga:

_____
_____
_____

Rasti trūkumai:

_____
_____
_____

Pasiūlymai dėl trūkumų šalinimo, Plano tikslinimo:

_____
_____
_____

Veiklos tęstinumo valdymo grupės vadovo ir ataskaitą parengusio asmens parašai:

_____ _____
(vardas, pavardė) (parašas)

_____ _____
(vardas, pavardė) (parašas)