PATVIRTINTA
Rokiškio rajono savivaldybės administracijos
direktoriaus 2022 m. gegužės 12 d.
įsakymu Nr. AV-512

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, 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.

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 informacinių technologijų specialistai.

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.

7.3. 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.

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

III. SAUGUS INFORMACIJOS TVARKYMAS

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

16. 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.

17. 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.

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

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

20. 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

21. 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.

22. 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.

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

23.1. 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;

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

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

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

25. 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 2022 m. gegužės 12 d.
įsakymu Nr. AV-512

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 Komunikacijos ir kultūros skyrių;

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)

PATVIRTINTA
Rokiškio rajono savivaldybės administracijos
direktoriaus 2022 m. gegužės 12 d.
įsakymu Nr. AV-512

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 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 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 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. 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 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.

III. APRAŠOMOSIOS NUOSTATOS

23. Kompiuterių tinklo fizinio ar loginio sujungimo schemas parengia sistemos administratoriai, saugo Komunikacijos ir kultūros skyrius.

24. 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.

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

IV. VALDYMO PLANO VEIKSMINGUMO PATIKRINIMAS

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

27. 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 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.

28. 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.

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

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	Veiklos atkūrimo grupė
	1.2. Įvertinkite pažeidimus ir padarytus nuostolius	Veiklos atkūrimo grupė
	1.3. Nustatykite, ar buvo prarasti kokie nors duomenys ar įranga	Veiklos atkūrimo grupė
	1.4. Jei būtina, perkelkite veiklą į atsargines patalpas	Veiklos atkūrimo grupė
	1.5. Jei yra sudarytos įrangos tiekimo sutartys, užsakykite reikalingą įrangą	Veiklos atkūrimo grupė
	1.6. Prireikus perskirstykite, kiek tai yra įmanoma, Savivaldybės išteklius, kad būtų atkurtas prioritetinių informacinės sistemos posistemių veikimas	Veiklos atkūrimo grupė
	1.7. Jei sutarčių nėra, inicijuokite ir vykdykite įrangos pirkimą	Veiklos atkūrimo grupė
	1.8. Įsigiję įrangą, atkurkite sistemos darbingumą	Veiklos atkūrimo grupė
	1.9. Jeigu būtina, atkurkite informacinės sistemos duomenis	Veiklos atkūrimo grupė
	1.10. Patikrinkite atkurtos informacinės sistemos veikimą ir duomenų teisingumą	Veiklos atkūrimo grupė
	1.11. Nustatykite, ar buvo prarasta kokia nors įranga ar duomenys	Veiklos atkūrimo grupė
2. Pavojingos medžiagos	2.1. Nustatykite, ar buvo prarasti kokie nors duomenys ar įranga	Veiklos atkūrimo grupė
	2.2. Jei būtina, perkelkite veiklą į atsargines patalpas	Veiklos atkūrimo grupė
	2.3. Jei yra sudarytos įrangos tiekimo sutartys, užsakykite reikalingą įrangą	Veiklos atkūrimo grupė
	2.4. Prireikus perskirstykite, kiek tai yra įmanoma, Savivaldybės išteklius, kad būtų atkurtas prioritetinių informacinės sistemos posistemių veikimas	Veiklos atkūrimo grupė
	2.5. Jei sutarčių nėra, inicijuokite ir vykdykite įrangos pirkimą	Veiklos atkūrimo grupė
	2.6. Įsigiję įrangą, atkurkite sistemos darbingumą	Veiklos atkūrimo grupė
	2.7. Jeigu būtina, atkurkite informacinės sistemos duomenis	Veiklos atkūrimo grupė

	2.8. Patikrinkite atkurtos informacinės sistemos veikimą ir duomenų teisingumą	Veiklos atkūrimo grupė
3. Gaisras	3.1. Esant galimybei, išjunkite ir užrakinkite visą įrangą	Veiklos atkūrimo grupė
	3.2. Likvidavus gaisrą įvertinkite pažeidimus ir padarytus nuostolius	Veiklos atkūrimo grupė
	3.3. Nustatykite, ar buvo prarasti kokie nors duomenys ar įranga	Veiklos atkūrimo grupė
	3.4. Jei būtina, perkelkite veiklą į atsargines patalpas	Veiklos atkūrimo grupė
	3.5. Prireikus perskirstykite, kiek tai yra įmanoma, Savivaldybės išteklius, kad būtų atkurtas prioritetinių informacinės sistemos posistemių veikimas	Veiklos atkūrimo grupė
	3.6. Jei yra sudarytos įrangos tiekimo sutartys, užsakykite reikalingą įrangą	Veiklos atkūrimo grupė
	3.7. Jei sutarčių nėra, inicijuokite ir vykdykite įrangos pirkimą	Veiklos atkūrimo grupė
	3.8. Įsigiję įrangą, atkurkite sistemos darbingumą	Veiklos atkūrimo grupė
	3.9. Jeigu būtina, atkurkite informacinės sistemos duomenis	Veiklos atkūrimo grupė
	3.10. Patikrinkite atkurtos informacinės sistemos veikimą ir duomenų teisingumą	Veiklos atkūrimo grupė
4. Patalpų užpuolimas	4.1. Nustatykite, ar buvo prarasti kokie nors duomenys ar įranga	Veiklos atkūrimo grupė
	4.2. Perkelkite veiklą į atsargines patalpas	Veiklos atkūrimo grupė
	4.3. Prireikus perskirstykite, kiek tai yra įmanoma, Savivaldybės išteklius, kad būtų atkurtas prioritetinių informacinės sistemos posistemių veikimas	Veiklos atkūrimo grupė
	4.4. Jei yra sudarytos įrangos tiekimo sutartys, užsakykite reikalingą įrangą	Veiklos atkūrimo grupė
	4.5. Jei sutarčių nėra, inicijuokite ir vykdykite įrangos pirkimą	Veiklos atkūrimo grupė
	4.6. Įsigiję įrangą, atkurkite sistemos darbingumą	Veiklos atkūrimo grupė
	4.7. Jeigu būtina, atkurkite informacinės sistemos duomenis	Veiklos atkūrimo grupė
	4.8. Patikrinkite atkurtos informacinės sistemos veikimą ir duomenų teisingumą	Veiklos atkūrimo grupė
5. Pagrindinės kompiuterinės įrangos praradimas, nepakenkiant patalpų funkcionalumui	5.1. Informuokite informacinės sistemos naudotojus apie veiklos sutrikimus	Veiklos atkūrimo grupė
	5.2. Įvertinkite nuostolius, nustatykite, kokia įranga prarasta	Veiklos atkūrimo grupė
	5.3. Prireikus perskirstykite, kiek tai yra įmanoma, Savivaldybės išteklius, kad būtų atkurtas prioritetinių informacinės sistemos posistemių veikimas	Veiklos atkūrimo grupė
	5.4. Jei yra sudarytos įrangos tiekimo sutartys,	Veiklos atkūrimo

	užsakykite reikalingą įrangą	grupė
	5.5. Jei sutarčių nėra, inicijuokite ir vykdykite įrangos pirkimą	Veiklos atkūrimo grupė
	5.6. Įsigiję įrangą, atkurkite sistemos darbingumą	Veiklos atkūrimo grupė
6. Pagrindinių darbuotojų praradimas, nepakenkiant patalpų ir įrangos funkcionalumui	6.1. Nustatykite, kokie gyvybiškai būtini įgūdžiai prarasti	Veiklos atkūrimo grupė
	6.2. Pasitelkite iš anksto numatytus pakaitinius darbuotojus, kad pakeistumėte trūkstamą personalą	Veiklos atkūrimo grupė
	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	Veiklos atkūrimo grupė
	7.2. Informuokite informacinės sistemos posistemio naudotojus apie veiklos sutrikimus	Veiklos atkūrimo grupė
	7.3. Tiksliai nustatykite prarastų duomenų apimtį ir praradimo priežastis	Veiklos atkūrimo grupė
	7.4. Nustatykite, ar paskutinės atsarginės kopijos yra patikimos	Veiklos atkūrimo grupė
	7.5. Atkurkite informacinės sistemos posistemio darbingumą	Veiklos atkūrimo grupė
	7.6. Nustatykite, ar atkurti duomenys yra patikimi	Veiklos atkūrimo grupė
	7.7. Jeigu duomenys buvo prarasti dėl saugumo spragų, pašalinkite jas	Veiklos atkūrimo grupė
	7.8. Praneškite informacinės sistemos posistemio, kurios duomenų nebuvo įmanoma atkurti, naudotojams, kad duomenis reikia įvesti iš naujo	Veiklos atkūrimo grupė
	7.9. Atkurkite informacinės sistemos posistemio naudotojų galimybę naudotis sistema, kad jie galėtų iš naujo įvesti prarastus duomenis	Veiklos atkūrimo grupė
	7.10. Atkurkite informacinės sistemos posistemio duomenis iš paskutinės, žinodami, kad ji gera, atsarginės kopijos;	Veiklos atkūrimo grupė
	7.11. Atkurkite visas informacinės sistemos posistemio naudotojų galimybes naudotis informacine sistema.	Veiklos atkūrimo grupė
8. Informacinės sistemos veiklos sutrikdymas dėl kibernetinių atakų	8.1. Informuokite informacinės sistemos naudotojus apie veiklos sutrikimus	Veiklos atkūrimo grupė
	8.2. Nustatykite trikdžių šaltinį	Veiklos atkūrimo grupė
	8.3. Nustatę, jog trikdžių šaltinis yra už Savivaldybės ribų, praneškite informacinės sistemos ryšio paslaugų teikėjui apie įvykį	Veiklos atkūrimo grupė
	8.4. Nustatykite, ar neprarasti arba nesugadinti informacinės sistemos duomenys	Veiklos atkūrimo grupė
	8.5. Pašalinę trikdžius, atkurkite sistemos	Veiklos atkūrimo

	darbingumą	grupė
	8.6. Jeigu būtina, atkurkite duomenis	Veiklos atkūrimo grupė
9. Būtinųjų komunalinių paslaugų teikimo sutrikimai	9.1. Informuokite informacinės sistemos naudotojus apie veiklos sutrikimus	Veiklos atkūrimo grupė
	9.2. Kreipkitės į komunalinių paslaugų teikėjus dėl sutrikimų pašalinimo	Veiklos atkūrimo grupė
	9.3. Organizuokite alternatyvų būtinųjų komunalinių paslaugų teikimą	Veiklos atkūrimo grupė
	9.4. Kai bus atnaujintas būtinųjų komunalinių paslaugų teikimas, atnaujinkite informacinės sistemos veikimą	Veiklos atkūrimo grupė
10. Ryšio sutrikimai	10.1. Informuokite informacinės sistemos naudotojus apie veiklos sutrikimus	Veiklos atkūrimo grupė
	10.2. Nustatykite ryšio paslaugų teikimo sutrikimo priežastis	Veiklos atkūrimo grupė
	10.3. Kreipkitės į ryšio paslaugų teikėjus dėl sutrikimų pašalinimo	Veiklos atkūrimo grupė
	10.4. Organizuokite alternatyvų gyvybiškai svarbių ryšio paslaugų teikimą	Veiklos atkūrimo grupė

Rokiškio rajono savivaldybės informacinės sistemos veiklos tęstinumo valdymo plano 2 priedas

ROKIŠKIO RAJONO SAVIVALDYBĖS 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 įvyko ir buvo nustatytas;	Saugumo įgaliotinis

	• 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 kibernetinio incidento tyrimo ataskaita, jei	Saugumo įgaliotinis

	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 informacinės sistemos veiklos tęstinumo valdymo plano 3 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 4 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 5 priedas

(Rizikos įvertinimo ataskaitos forma)

TVIRTINU
Direktorius

ROKIŠKIO RAJONO SAVIVALDYBĖS 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)

PATVIRTINTA
Rokiškio rajono savivaldybės administracijos
direktoriaus 2022 m. gegužės 12 d.
įsakymu Nr. AV-512

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

16.1. Administracijos Teisės 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.

17. Papildomi reikalavimai Administratoriaus slaptažodžiui:

17.1. slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius;

17.2. slaptažodį turi sudaryti ne mažiau kaip 12 simbolių.

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

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

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

20. Pasirašytos instrukcijos saugomos Administracijos Teisės ir personalo skyriuje.

PATVIRTINTA
Rokiškio rajono savivaldybės administracijos
direktoriaus 2022 m. gegužės 12 d.
įsakymu Nr. AV-512

ROKIŠKIO RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Rokiškio rajono savivaldybės administracijos informacinių sistemų duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja informacinių sistemų ir kitų informacinių technologijų priemonių, kurių valdytojas yra Rokiškio rajono savivaldybės administracija (toliau – IS), elektroninės informacijos saugos ir kibernetinio saugumo politiką.

2. Saugos nuostatuose vartojamos sąvokos atitinka sąvokas, apibrėžtas Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos vietos savivaldos įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas).

3. IS elektroninės informacijos saugumo ir kibernetinio saugumo užtikrinimo tikslas – apsaugoti IS tvarkomos elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą.

4. IS elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

4.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų IS elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti, įgyvendinimas ir kontrolė;

4.2. IS veiklos tęstinumo užtikrinimas;

4.3. IS naudotojų mokymas.

5. Saugos nuostatai privalomi Rokiškio rajono savivaldybės administracijai, įmonės kodas 188772248, Respublikos g. 94, LT-42136, Rokiškis, IS naudotojams, IS saugos įgaliotiniui ir IS administratoriui, IS funkcionuoti reikalingų paslaugų teikėjams.

6. IS valdytojas ir tvarkytojas yra Rokiškio rajono savivaldybės administracija.

7. IS valdytojas atsako už IS elektroninės informacijos saugos (kibernetinio saugumo) politikos formavimą, politikos įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą bei vykdo šias funkcijas:

7.1. rengia ir tvirtina IS elektroninės informacijos saugos (kibernetinio saugumo) politiką įgyvendinančius dokumentus;

7.2. kontroliuoja, kaip laikomasi IS elektroninės informacijos saugos (kibernetinio saugumo) politiką įgyvendinančių dokumentų ir kitų teisės aktų, reglamentuojančių elektroninės informacijos tvarkymo teisėtumą ir saugos valdymą;

7.3. priima sprendimus dėl IS techninių ir programinių priemonių, būtinų IS elektroninės informacijos saugai (kibernetiniam saugumui) užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

7.4. skiria IS saugos įgaliotinį (toliau – Saugumo įgaliotinis);

7.5. skiria IS administratorių (toliau – administratorius);

7.6. vykdo kitas Saugos nuostatuose, saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą (kibernetinį saugumą), IS valdytojui priskirtas funkcijas.

8. IS tvarkytojas atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimo užtikrinimą ir laikymąsi Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka bei vykdo šias funkcijas:

8.1. pagal kompetenciją įgyvendina IS elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus;

8.2. užtikrina Saugos nuostatų, saugos politiką įgyvendinančių dokumentų ir IS valdytojo priimtų teisės aktų, susijusių su IS elektroninės informacijos sauga (kibernetiniu saugumu), tinkamą įgyvendinimą;

8.3. pagal kompetenciją užtikrina IS elektroninės informacijos saugą (kibernetinį saugumą);

8.4. prižiūri IS duomenų bazių valdymo sistemas, taikomųjų programų sistemas, ugniasienes, įsilaužimų aptikimo sistemas, elektroninės informacijos perdavimo tinklus, kompiuterius, operacines sistemas ir kitus IS komponentus, užtikrina jų veikimą;

8.5. vykdo kitas Saugos nuostatuose, saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą (kibernetinį saugumą), IS tvarkytojui priskirtas funkcijas.

9. Saugos įgaliotinio funkcijos ir atsakomybė:

9.1. teikia IS valdytojo vadovui pasiūlymus dėl:

9.1.1. administratoriaus paskyrimo ir reikalavimų administratoriui nustatymo;

9.1.2. Saugos nuostatų ir saugos politiką įgyvendinančių dokumentų priėmimo arba keitimo;

9.1.3. informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

9.2. koordinuoja elektroninės informacijos saugos incidentų tyrimą, išskyrus atvejus, kai šią funkciją atlieka IS valdytojo vadovo įsakymu sudaryta informacijos saugos darbo grupė;

9.3. organizuoja IS rizikos vertinimą;

9.4. atlieka Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas), nustatytas asmens, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, funkcijas;

9.5. supažindina administratorių ir IS naudotojus su Saugos nuostatų, saugos politiką įgyvendinančių dokumentų reikalavimais ir atsakomybe už reikalavimų nesilaikymą;

9.6. teikia administratoriui ir IS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos (kibernetinio saugumo) politikos įgyvendinimu;

9.7. organizuoja IS naudotojų mokymus elektroninės informacijos saugos (kibernetinio saugumo) klausimais, informuoja juos apie elektroninės informacijos saugos problemas;

9.8. vykdo kitas Saugos nuostatuose, saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą (kibernetinį saugumą), saugos įgaliotiniui ir asmeniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą, nustatytas funkcijas.

10. Administratoriaus funkcijos ir atsakomybė:

10.1. užtikrina IS komponentų (kompiuterių, tarnybinių stočių, operacinių sistemų, taikomųjų programų, duomenų bazės valdymo sistemų, ugniasienių, įsilaužimo aptikimo sistemų ir kt.) tinkamą veikimą ir priežiūrą;

10.2. parengia ir diegia saugos priemones bei užtikrina jų atitiktį Saugos nuostatų ir saugos politiką įgyvendinančių dokumentų reikalavimams;

10.3. atsako už IS naudotojų registravimą ir prieigos teisių nustatymą;

10.4. pagal kompetenciją vertina IS naudotojų pasirengimą dirbti su IS;

10.5. dalyvauja vykdant saugumo reikalavimų įgyvendinimo stebėseną;

10.6. nuolat teikia saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę, neveikiančias ar netinkamai veikiančias IS elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo priemones, Saugos nuostatų ir saugos politiką įgyvendinančių

dokumentų pažeidimus, registruoja elektroninės informacijos saugos incidentus ir apie juos informuoja saugos įgaliotinį, teikia siūlymus dėl elektroninės informacijos saugos incidentų pašalinimo;

10.7. daro IS elektroninės informacijos atsargines kopijas ir atsako už kopijų saugojimą;

10.8. pagal kompetenciją teikia siūlymus dėl IS palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

10.9. atlieka kitas IS tvarkytojo, saugos įgaliotinio pavestas, Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

11. Teisės aktai, kuriais vadovaujamasi tvarkant IS elektroninę informaciją ir užtikrinant jos saugą:

11.1. 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);

11.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

11.3. Kibernetinio saugumo įstatymas;

11.4. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

11.5. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“;

11.6. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas;

11.7. Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymas Nr. V-941 „Dėl techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

11.8. kiti teisės aktai, reglamentuojantys elektroninės informacijos saugą (kibernetinį saugumą) bei asmens duomenų tvarkymą, IS valdytojo ir tvarkytojo veiklą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

12. IS tvarkomos elektroninės informacijos kategorija – mažiausios svarbos informacija. IS tvarkomos elektroninės informacijos priskyrimo mažiausios svarbos informacijai kriterijus – Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Klasifikavimo gairių aprašas), 10 punktas, t. y. IS tvarkoma informacija nepatenka į Klasifikavimo gairių aprašo 6.1–6.3 papunkčiuose nurodytas kategorijas;

13. IS pagal tvarkomos informacijos svarbą priskiriama ketvirtai kategorijai. IS priskyrimo ketvirtai kategorijai kriterijus – Klasifikavimo gairių aprašo 12.4. punktas, t. y. IS tvarkoma mažiausios svarbos informacija.

14. Saugumo įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro prie Lietuvos Respublikos krašto apsaugos ministerijos interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, kasmet organizuoja rizikos vertinimą. Prireikus (po esminių organizacinių ar sisteminių pokyčių, nustačius naujų rizikos veiksnių ar pan.) Saugumo įgaliotinis gali organizuoti neeilinį rizikos vertinimą. IS valdytojo vadovo rašytiniu pavedimu rizikos

vertinimą gali atlikti pats Saugumo įgaliotinis. Rizikos vertinimas gali būti atliekamas kartu su informacinių technologijų saugos atitikties vertinimu.

15. Rizikos vertinimas įforminamas rizikos vertinimo ataskaitoje. Rizikos vertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Rizikos vertinimo ataskaita pateikiama IS valdytojui.

16. Svarbiausi rizikos veiksniai yra šie:

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

16.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis IS elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

16.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

17. Rizikos veiksniai rizikos vertinimo ataskaitoje turi būti išdėstyti pagal prioritetus ir priimtiną rizikos lygį.

18. Atsižvelgdamas į rizikos vertinimo ataskaitą, IS valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

19. Siekiant įvertinti IS saugos dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, Saugumo įgaliotinis ne rečiau kaip vieną kartą per metus organizuoja informacinių technologijų saugos atitikties vertinimą, kurio metu:

19.1. įvertinama saugos politiką įgyvendinančių dokumentų ir realios informacijos saugos situacijos atitiktis;

19.2. inventorizuojama IS techninė ir programinė įranga;

19.3. patikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų IS naudotojų kompiuterinių darbo vietų, visose tarnybinėse stotyse įdiegtos programos ir jų sąranga;

19.4. įvertinama IS naudotojams suteiktų teisių ir vykdomų funkcijų atitiktis;

19.5. įvertinamas pasirengimas užtikrinti IS veiklos tęstinumą įvykus saugos incidentui.

20. Atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama IS valdytojo vadovui. Įvertinus informacinių technologijų saugos atitikties vertinimo ataskaitą, prireikus rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato IS valdytojo vadovas.

21. IS atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus.

22. Elektroninės informacijos saugos (kibernetinio saugumo) priemonės (techninės, programinės, organizacinės ir kitos elektroninės informacijos saugos (kibernetinio saugumo) priemonės) parenkamos vadovaujantis šiais priemonių parinkimo principais:

22.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

22.2. informacijos saugos priemonės diegimo kaina turi būti adekvati saugomos informacijos vertei;

22.3. kur galima, turi būti įdiegiamos prevencinės, detekcinės ir korekcinės informacijos saugos (kibernetinio saugumo) priemonės.

23. Rizikos vertinimo ataskaita, rizikos įvertinimo ir rizikos valdymo priemonių plano kopija, informacinių technologijų saugos atitikties vertinimo ataskaita, pastebėtų trūkumų šalinimo plano kopija ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikiamos Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

24. Organizaciniai ir techniniai elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai nustatomi pagal Saugos nuostatų 13 punkte nustatytą IS svarbos kategoriją ir vadovaujantis Saugos nuostatų 11 punkte nurodytais teisės aktais.

25. Organizacinių ir techninių elektroninės informacijos saugos (kibernetinio saugumo) priemonių užtikrinimas turi būti grindžiamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos elektroninės informacijos saugai (kibernetiniam saugumui), rizikos vertinimu, atsižvelgiant į naujausius technikos laimėjimus.

26. Organizaciniai ir techniniai elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai detalizuojami saugos politiką įgyvendinančiuose dokumentuose.

27. Programinės įrangos, skirtos IS nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir panašiai) apsaugoti, naudojimo nuostatos ir jos atnaujinimo reikalavimai:

27.1. Tarnybinių stočių ir kompiuterinėse darbo vietose turi būti įdiegtos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės, kurios atnaujinamos automatiniu būdu ne rečiau kaip kartą per parą.

27.2. Naudojamos priemonės, turinčios apsaugos mechanizmus, blokuojančius kenkimo programų bandymus panaikinti apsaugas nuo kenkimo programų.

28. Detalios programinės įrangos, skirtos apsaugoti IS nuo kenksmingos programinės įrangos, naudojimo nuostatos ir jos atnaujinimo reikalavimai nustatomi IS saugaus elektroninės informacijos tvarkymo taisyklėse.

29. Programinės įrangos, įdiegtos kompiuteriuose ir tarnybinėse stotyse, naudojimo nuostatos:

29.1. turi būti naudojama tik legali ir IS naudotojų funkcijoms vykdyti ir IS administruoti būtina programinė įranga;

29.2. programinė įranga turi būti nuolatos atnaujinama laikantis gamintojo reikalavimų;

29.3. turi būti įdiegta prieigos prie elektroninės informacijos per registravimą, teisių suteikimą ir slaptažodžius sistema;

29.4. IS naudotojams draudžiama patiems diegti bet kokią programinę įrangą.

30. Kompiuterių tinklo filtravimo įrangos pagrindinės naudojimo nuostatos:

30.1. Elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienes, ugniasienių įvykių žurnalai turi būti reguliariai analizuojami;

30.2. IS programinė įranga privalo turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų;

30.3. IS perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių IS naudotojų kompiuterinę įrangą nuo kenksmingo kodo;

30.4. IS elektroninės informacijos apsaugai naudojama įsilaužimų prevencijos sistema – tinklo saugumo prietaisas, įrengiamas IS prieigose ir skirtas aptikti tinklų ir (arba) sistemų kenksmingą veiklą, fiksuoti informaciją apie šią veiklą, bandyti blokuoti (sustabdyti) šią veiklą ir apie tai pranešti administratoriui.

31. Detalios kompiuterių tinklo filtravimo įrangos naudojimo nuostatos nustatomos IS saugaus elektroninės informacijos tvarkymo taisyklėse.

32. Leistinos kompiuterių naudojimo ribos:

32.1. stacionarūs ir nešiojamieji IS naudotojų kompiuteriai ir kiti mobilieji įrenginiai turi būti naudojami tik tiesioginėms pareigoms atlikti. Iš kompiuterių, kurie perduodami remontuoti ar techninei priežiūrai atlikti, turi būti pašalinti visi IS duomenys ir informacija;

32.2. nešiojamuosiuose kompiuteriuose ir kituose mobiliuosiuose įrenginiuose turi būti taikomos papildomos saugos priemonės – elektroninės informacijos šifravimas ir prisijungimo ribojimas;

32.3. nuotoliniu būdu jungiantis prie IS yra naudojama VPN technologija;

32.4. IS naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo.

33. Metodai, kuriais užtikrinamas saugus elektroninės informacijos teikimas ir (ar) gavimas:

33.1. IS elektroninė informacija automatiniu būdu perduodama, koduotu kanalu TCP/IP protokolu, prieiga prie duomenų ribojama pagal IP adresą;

33.2. IS elektroninė informacija perduodama realiu laiku arba asinchroniniu režimu pagal duomenų teikimo ir gavimo sutartis, kuriose nustatytos perduodamų duomenų specifikacijos, perdavimo sąlygos ir tvarka;

33.3. IS elektroninė informacija automatiniu būdu teikiama XML formatu.

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

34.1. Elektroninės informacijos atsarginės kopijos daromos automatiniu būdu kartą per parą ir saugomos paskutinių 14 dienų atsarginės kopijos. Kopijos turi būti saugomos kitoje patalpoje, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota. Elektroninė informacija kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo kopijų).

34.2. Prireikus atkurti kopijas teisę tam turi tik administratorius. Periodiškai, bet ne rečiau kaip kartą per pusmetį, turi būti atliekami elektroninės informacijos atkūrimo iš atsarginių kopijų bandymai. Patekimas į patalpas, kuriose saugomos atsarginės elektroninės informacijos kopijos, turi būti kontroliuojamas.

35. Detali kopijų darymo ir saugojimo tvarka nustatoma IS saugaus elektroninės informacijos tvarkymo taisyklėse.

36. Organizaciniai ir techniniai elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai detalizuojami saugos politiką įgyvendinančiuose dokumentuose.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

37. Saugumo įgaliotinis privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, tobulinti elektroninės informacijos saugos (kibernetinio saugumo) srities kvalifikaciją, savo darbe vadovautis Lietuvos Respublikos ir Europos Sąjungos teisės aktų, reglamentuojančių elektroninės informacijos saugą, nuostatomis, turėti atitinkamą kvalifikaciją įgyvendinti elektroninės informacijos saugos (kibernetinio saugumo) politiką, taip pat turėti darbo su duomenų bazėmis, operacinėmis sistemomis, taikomosiomis programomis patirties.

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

39. Administratorius privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, mokėti užtikrinti IS ir tvarkomos elektroninės informacijos saugą

(kibernetinį saugumą), administruoti ir prižiūrėti IS komponentus (stebėti komponentų veikimą, atlikti jų profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, sugebėti užtikrinti komponentų nepertraukiamą funkcionavimą ir pan.), būti susipažinęs su saugos politiką įgyvendinančiais dokumentais, darbo saugos taisyklėmis.

40. IS naudotojai privalo turėti pagrindinius darbo kompiuteriu, taikomosiomis programomis įgūdžius, mokėti tvarkyti elektroninę informaciją, būti susipažinę su teisės aktais, reglamentuojančiais asmens duomenų tvarkymą, elektroninės informacijos tvarkymą. IS naudotojai, tvarkantys duomenis ir informaciją, privalo saugoti jų paslaptį. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą.

41. Saugos įgaliotinio, administratoriaus, IS naudotojų kvalifikacija turi atitikti reikalavimus, nustatytus jų pareiginiuose nuostatuose ar pareigybės aprašyme.

42. IS naudotojų mokymą ir informavimą elektroninės informacijos saugos (kibernetinio saugumo) klausimais planuoja bei organizuoja Saugumo įgaliotinis. IS naudotojai apie elektroninės informacijos saugos (kibernetinio saugumo) problemas, gerąją praktiką elektroninės informacijos saugos (kibernetinio saugumo) srityje informuojami siunčiant priminimus, konsultuojant elektroniniu paštu ar per dokumentų valdymo sistemą, rengiant ir pateikiant atmintines, organizuojant teminius seminarus ir mokymus ir kitais būdais.

43. Mokymai elektroninės informacijos saugos (kibernetinio saugumo) klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), saugos įgaliotinio, IS naudotojų poreikius.

44. Mokymai gali būti vykdomi tiesioginiu (pvz., paskaitos, seminarai, konferencijos ir kt. teminiai renginiai) ar nuotoliniu būdu (pvz., vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir pan.).

45. Mokymai IS naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per metus.

46. Mokymai saugos įgaliotiniui ir administratoriui turi būti organizuojami pagal poreikį.

V SKYRIUS
IS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

47. Tvarkyti IS elektroninę informaciją gali tik IS naudotojai, kurie yra susipažinę su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ir sutikę laikytis jų reikalavimų. IS naudotojai atsako už IS ir tvarkomos elektroninės informacijos saugą (kibernetinį saugumą) pagal savo kompetenciją.

48. IS naudotojus su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ir atsakomybe už jų reikalavimų nesilaikymą supažindina Saugumo įgaliotinis.

49. IS naudotojų supažindinimas su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ar jų pakeitimais turi būti vykdomas šiais atvejais:

49.1. prieš suteikiant naudotojams prieigą prie IS;

49.2. pakeitus Saugos nuostatus ir (ar) saugos politiką įgyvendinančius dokumentus;

49.3. periodiškai, mokymų elektroninės informacijos saugos (kibernetinio saugumo) temomis metu.

50. IS naudotojų supažindinimo su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais tvarka nustatyta IS naudotojų administravimo taisyklėse.

51. IS naudotojai, administratorius ir Saugumo įgaliotinis, pažeidę Saugos nuostatų, saugos politiką įgyvendinančių dokumentų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

52. Saugos dokumentai persvarstomi (peržiūrimi) atlikus rizikos įvertinimą ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems IS valdytojo veiklos pokyčiams, bet ne rečiau kaip kartą per metus.
