LIETUVOS RESPUBLIKOS
RYŠIŲ REGULIAVIMO TARNYBOS
DIREKTORIUS

ĮSAKYMAS
DĖL LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBOS ELEKTRONINIŲ PASLAUGŲ INFORMACINĖS SISTEMOS SAUGOS POLITIKĄ ĮGYVENDINANČIŲ DOKUMENTŲ PATVIRTINIMO

2017 m. gruodžio 22 d. Nr. 1V-1291
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų, 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“, 7 ir 8 punktais,

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

1.1. Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisykles;

1.2. Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos veiklos tęstinumo valdymo planą;

1.3. Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos naudotojų administravimo taisykles.

2. N u r o d a u paskelbti šį įsakymą Teisės aktų registre.

Direktorius Feliksas Dobrovolskis

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2017 m. gruodžio 8 d. raštu Nr. 1D-6456

PATVIRTINTA
Lietuvos Respublikos
ryšių reguliavimo tarnybos direktoriaus
2017 m. gruodžio 22 d.
įsakymu Nr. 1V-1291

LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBOS ELEKTRONINIŲ PASLAUGŲ INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) nustato minimalius Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinėje sistemoje (toliau – EPIS) tvarkomos elektroninės informacijos saugos reikalavimus.

2. Taisyklės privalomos EPIS naudotojams, EPIS administratoriui, EPIS duomenų valdymo įgaliotiniui ir EPIS saugos įgaliotiniui.

3. Už Taisyklių įgyvendinimo organizavimą ir kontrolę atsako EPIS saugos įgaliotinis.

4. Taisyklėse vartojamos sąvokos apibrėžtos 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“.

5. EPIS tvarkoma elektroninė informacija, nurodyta Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos nuostatų, patvirtintų Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2016 m. rugsėjo 26 d. įsakymu Nr. 1V-1005 „Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos nuostatų patvirtinimo“, (toliau – EPIS nuostatai) III skyriuje.

6. EPIS administratorius atsakingas už EPIS administravimą, duomenų bazės atkūrimą ir priežiūrą, paslaugų prieinamumo užtikrinimą, klasifikatorių, EPIS naudotojų duomenų ir jiems suteiktų teisių tvarkymą.

7. EPIS naudotojai atsakingi už duomenų, nurodytų EPIS nuostatų 13 punkte, išskyrus nurodytus Taisyklių 6 punkte, tvarkymą.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

8. Bendrieji techniniai EPIS elektroninės informacijos saugos reikalavimai:

8.1. Periodiškai (kartą per du metus) turi būti atliekamas EPIS informacinių technologijų saugos atitikties vertinimas.

8.2. EPIS turi registruoti duomenų bazės informacijos ir tarnybinių stočių operacinės sistemos pakeitimus, fiksuoti paskutinį elektroninės informacijos pakeitimą atlikusį EPIS naudotoją ir tokio pakeitimo laiką.

8.3. EPIS priežiūros funkcijos turi būti vykdomos naudojant atskirą tam skirtą administratoriaus identifikatorių, kuriuo naudojantis negalima atlikti kitų EPIS naudotojų funkcijų.

8.4. Kiekvienas EPIS naudotojas turi būti unikaliai identifikuojamas – EPIS naudotojas patvirtina savo tapatybę skaitmeniniu kvalifikuotu sertifikatu.

8.5. EPIS naudotojui ar EPIS administratoriui baigus darbą su EPIS, turi būti imamasi priemonių, kad su EPIS elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo EPIS, saugi sertifikato laikmena atjungiama nuo kompiuterinės įrangos, uždaroma programinė įranga, įjungiama ekrano užsklanda su slaptažodžiu.

8.6. EPIS naudotojui neatliekant jokių veiksmų 60 min., EPIS naudotojo paskyra automatiškai atjungiama ir naudotis EPIS galima tik pakartojus EPIS naudotojo tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus.

8.7. EPIS turi perspėti EPIS administratorių, kai EPIS tarnybinėse stotyse laisvos operatyviosios atminties ar laisvos vietos diske sumažėja iki nustatytos pavojingos ribos, taip pat kai ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja.

8.8. EPIS turi būti įdiegtos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemonės (filtrai).

8.9. Tarnybinių stočių įvykių žurnaluose (angl. *event log*) turi būti fiksuojami ir 1 mėnesį saugomi duomenys apie: EPIS įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis ir prieiti prie EPIS elektroninės informacijos, kitus svarbius saugai įvykius, nurodant EPIS naudotojo identifikatorių ir įvykio laiką. Ši informacija analizuojama įvykus elektroninės informacijos saugos incidentui.

8.10. EPIS veiklos atkūrimas turi būti atliekamas vadovaujantis EPIS veiklos tęstinumo valdymo planu.

9. EPIS kompiuterinės įrangos saugos priemonės:

9.1. Tarnybinės stotys ir svarbiausi elektroninės informacijos perdavimo tinklo mazgai turi įtampos filtrą ir nenutrūkstamo maitinimo šaltinį. Nenutrūkstamo maitinimo šaltinis užtikrina tarnybinių stočių veikimą ne trumpiau kaip 30 min.

9.2. Tarnybinės stotys, svarbiausi elektroninės informacijos perdavimo tinklo mazgai ir ryšio linijos yra dubliuojami ir jų techninė būklė nuolat stebima; visa EPIS kompiuterinė įranga apskaitoma specialiame žurnale, nurodant įrangos aparatinę sąranką, EPIS naudotoją, jo darbo vietą ir telefono numerius.

9.3. Už Lietuvos Respublikos ryšių reguliavimo tarnybos (toliau – Tarnyba) patalpose esančią kompiuterinę įrangą atsakingas Tarnybos Administracinio departamento Informacinių technologijų skyrius.

9.4. EPIS kompiuterinės įrangos gedimai užfiksuojami žurnale.

9.5. Visose EPIS tarnybinėse stotyse ir kompiuterizuotose darbo vietose yra įdiegta ir reguliariai atnaujinama virusų ir kenkimo kodo aptikimo ir šalinimo programinė įranga, skirta kompiuteriams ir laikmenoms tikrinti. Kompiuterizuotose darbo vietose naudojamos centralizuotai valdomos kenkimo programinės įrangos aptikimo priemonės, kurios reguliariai atnaujinamos.

10. Sisteminės ir taikomosios EPIS programinės įrangos saugos priemonės:

10.1. Operacinei sistemai ir kitai programinei įrangai operatyviai atnaujinti naudojama WSUS (angl. *Windows Server Update Services*) tarnybinė stotis. Įdiegiami tik gamintojų rekomenduojami naujiniai.

10.2. Naudojama tik teisėtai įgyta, patikimų gamintojų programinė įranga.

10.3. Programinės įrangos diegimą, konfigūravimą ir šalinimą atlieka tik EPIS administratorius.

10.4. Programinė įranga prižiūrima laikantis gamintojo rekomendacijų.

10.5. Programinės įrangos testavimas atliekamas naudojant atskirą testavimo aplinką.

11. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

11.1 EPIS tarnybinės stotys, EPIS naudotojų kompiuterizuotos darbo vietos ir kita kompiuterinė įranga, įjungta į elektroninės informacijos perdavimo tinklą, yra atskirta nuo viešųjų elektroninių ryšių tinklų naudojant užkardas.

11.2. EPIS elektroninės informacijos perdavimo tinklas yra segmentuotas pagal EPIS sudedamųjų dalių atliekamas funkcijas ir turi priskirtus IP adresų intervalus:

11.2.1. Tarnybinių stočių tinklą sudaro taikomųjų programų tarnybinės stotys.

11.2.2. EPIS naudotojų kompiuterizuotų darbo vietų tinklus sudaro nutolusių EPIS naudotojų kompiuterinės darbo vietos ir kompiuterinė įranga.

11.2.3. EPIS kūrimo, tobulinimo ir testavimo tinklą sudaro testavimo darbams naudojamos tarnybinės stotys ir duomenų bazių testavimo tarnybinės stotys.

11.2.4. Administratorių tinklą sudaro darbuotojų, turinčių EPIS ir (ar) tarnybinių stočių administratoriaus teises, kompiuterizuotos darbo vietos.

11.2.5. Elektroninės informacijos perdavimo tinklo aptarnavimo ir saugumo potinklį sudaro tinklo stebėjimo, aptarnavimo, antivirusinių sistemų tarnybinės stotys.

11.2.6. Demilitarizuotos zonos tinklą sudaro tarnybinės stotys, kurios turi ryšį su viešaisiais elektroninių ryšių tinklais.

11.3. Demilitarizuota zona tiek nuo išorinio, tiek nuo vidinio elektroninės informacijos perdavimo tinklo atskirta užkardomis.

11.4. Nutolę EPIS naudotojai perduoda informaciją naudodami saugias ryšio linijas.

11.5. Nutolę EPIS naudotojai, duomenis perduodantys ir gaunantys viešaisiais elektroninių ryšių tinklais, perduodamų duomenų konfidencialumą užtikrina naudodami duomenų šifravimą arba virtualųjį privatųjį tinklą.

11.6. EPIS taikoma trijų lygių elektroninės informacijos perdavimo tinklo apsauga – išorinis tinklas, taikomosios programos, duomenų bazės, kiekvieną iš lygių atskiriant užkardomis.

11.7. Jungimasis prie EPIS iš viešųjų elektroninių ryšių tinklų yra griežtai kontroliuojamas ir atliekamas tik per tarpines tarnybines stotis.

11.8. Keitimasis informacija su kitais registrais ir informacinėmis sistemomis galimas tik naudojant saugius šifruotus ryšio kanalus (VPN, SSL) ir tarpines tarnybines stotis.

11.9. Elektroninės informacijos perdavimo tinklai stebimi šia tvarka:

11.9.1. Visi tinklo įrenginiai, turintys paprastojo tinklo stebėjimo protokolo (angl. *Simple Network Management Protocol, SNMP*) parinktį, stebimi tinklo priežiūros sistemos ir, kilus nesklandumų, automatiškai praneša apie problemą atsakingiems darbuotojams.

11.9.2. Visi ryšių kanalai stebimi tinklo priežiūros sistemos ir, esant sutrikimų arba didelei apkrovai, automatiškai praneša apie problemą atsakingiems darbuotojams.

11.9.3. EPIS duomenų gavėjams duomenys viešaisiais elektroninių ryšių tinklais perduodami tik hipertekstų persiuntimo protokolu (angl. *Hypertext Transfer Protocol, HTTPS*).

12. Patalpų ir aplinkos saugumo užtikrinimo priemonės:

12.1. Tarnybos pastate įrengta elektroninė perimetro kontrolės sistema. Tarnybinių stočių patalpos turi atskirą elektroninę perimetro kontrolės sistemą.

12.2. Tarnybos pastate įrengta atskirų patalpų apsaugos signalizacija, kurios signalai pasibaigus darbo dienai, taip pat poilsio ir švenčių dienomis persiunčiami patalpas saugančiai saugos tarnybai. Visose patalpose įrengti įsilaužimo davikliai prijungti prie pastato signalizacijos ir apsaugos tarnybos.

12.1.3. Kiekvienas darbuotojas turi asmeninę magnetinę kortelę ir įeidamas arba išeidamas pasižymi įėjimo punktuose.

12.1.4. Visi darbuotojų įėjimai į patalpas ir išėjimai fiksuojami ir saugomi elektronine forma.

12.1.5. Lankytojams privalomai išduodamos svečio elektroninės kortelės. Už apsilankymą atsakingas darbuotojas pasirašo įėjimo žurnale už kiekvieną lankytoją.

12.1.6. Po 18 val. vakaro ir nedarbo dienomis į pastatą patekti gali tiktai specialius leidimus turintys darbuotojai.

12.1.7. Tarnybinių stočių patalpos sienos sumūrytos iš plytų ar blokelių, lubos pagamintos iš gelžbetonio.

12.1.8. Tarnybinių stočių patalpos durys atsparios laužimui, nedegios, savaime užsidarančios. Duryse yra viena cilindrinė spyna ir viena plokštelinė spyna.

12.1.9. Į tarnybinių stočių patalpas gali patekti tik Tarnybos direktoriaus patvirtintame sąraše išvardyti darbuotojai. Valymas, elektros tinklo priežiūra, patalpų remonto ir kiti darbai atliekami tik dalyvaujant darbuotojui, turinčiam leidimą patekti į tarnybinių stočių patalpas.

12.1.10. Tarnybinių stočių patalpa turi alternatyvų elektros energijos tiekimo šaltinį.

12.1.11. Nenutrūkstamo maitinimo šaltinis vieną kartą per mėnesį tikrinamas imituojant elektros energijos dingimą.

12.1.12. Nenutrūkstamo maitinimo šaltinis automatiškai įsijungia dingus elektros įtampai, o sistema automatiškai informuoja atsakingus darbuotojus apie gedimą.

12.1.13. Aplinkos drėgnis tarnybinių stočių patalpoje nuolat stebimas automatizuotos sistemos. Rodmenims padidėjus arba sumažėjus daugiau nei technikos gamintojo nurodytos leistinos normos, sistema automatiškai informuoja atsakingus darbuotojus apie nesklandumus.

12.1.14. Tarnybinių stočių patalpoje įrengta gaisro gesinimo dujomis sistema.

12.1.15. Kitose patalpose prieinamoje vietoje įrengtos nešiojamosios gaisro gesinimo priemonės ir gaisriniai čiaupai.

12.1.16. Visos priešgaisrinės sistemos ir priemonės periodiškai tikrinamos kas 1 mėnesį. Patikros užfiksuojamos žurnale, kuriame nurodoma patikros data, patikrinimo lygis, asmens, atlikusio patikrą, vardas, pavardė ir parašas.

12.1.17. Už priešgaisrinę saugą atsakingas Tarnybos Bendrųjų reikalų ir personalo skyriaus administratorius.

12.1.18. Tarnybinių stočių patalpos raktai saugomi seife. Atsarginiai tarnybinių stočių patalpos raktai saugomi kitame nei pagrindiniai raktai pastate.

12.1.19. Ribojama fizinė prieiga prie tinklo kabelių, skirstytuvų, atšakų, kartotuvų ir antgalių.

12.1.20. Kompiuterių ryšio linijos apsaugotos nuo elektros išlydžių, perkūnijos ir elektros linijų avarijų naudojant apsauginius įtaisus su įžeminimo tašku.

13. Kitos priemonės, naudojamos elektroninės informacijos saugai užtikrinti:

13.1. EPIS naudotojams suteikiama prieigos teisė atlikti veiksmus EPIS naudotojų administravimo taisyklėse nustatyta tvarka.

13.2. Elektroniniuose žurnaluose fiksuojami EPIS naudotojo veiksmai su EPIS duomenimis.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

14. Saugaus elektroninės informacijos keitimo, atnaujinimo, įvedimo ir naikinimo užtikrinimo tvarka:

14.1. EPIS tvarkomus duomenis įvesti, keisti, atnaujinti, naikinti gali EPIS naudotojas pagal jam EPIS naudotojų administravimo taisyklių nustatyta tvarka suteiktas teises.

14.2. EPIS duomenys gali būti įvesti, pakeisti, atnaujinti, sunaikinti tik turint tam teisinį pagrindą.

14.3. Duomenų įvedimas, keitimas, atnaujinimas, naikinimas fiksuojami elektroniniuose žurnaluose, nurodant EPIS naudotoją, darbo laiką, prisijungimo prie EPIS datą, atliktus veiksmus.

15. EPIS naudotojų veiksmų fiksavimo tvarka:

15.1. EPIS naudotojo veiksmai su EPIS duomenimis automatiškai registruojami elektroniniuose žurnaluose.

15.2. EPIS administratorius gali peržiūrėti duomenų sukūrimo, keitimo, atnaujinimo ar naikinimo veiksmus pagal atskirą objektą (pvz., dokumentą, klasifikatorių), naudotoją, instituciją, laiko intervalą.

16. Atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarka:

16.1. EPIS duomenų bazių ir archyvų valdymas organizuojamas atsižvelgiant į EPIS nuostatų 32 punkto reikalavimus.

16.2. EPIS atsarginių kopijų darymo ir atkūrimo reikalavimai aprašyti Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos saugos nuostatų, patvirtintų Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2016 m. rugsėjo 26 d. įsakymu Nr. 1V-1006 „Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos saugos nuostatų patvirtinimo“, 27 punkte.

16.3. Visų EPIS duomenų kopija saugoma atskiroje nuo EPIS tarnybinių stočių patalpoje.

16.4. EPIS duomenis iš atsarginės kopijos turi teisę atkurti EPIS administratorius, prieš tai įsitikinęs, kad toks atkūrimas nesugadins esamų duomenų.

16.5. Apie EPIS duomenų atkūrimą EPIS administratorius privalo informuoti EPIS saugos įgaliotinį.

16.6. Visiškas EPIS atkūrimas iš atsarginės kopijos turi užtrukti ne ilgiau kaip 24 valandas.

17. Elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo nustatymo tvarka:

17.1. EPIS naudotojai, pastebėję neteisėtą duomenų kopijavimą, keitimą, naikinimą, perdavimą ar kitus saugos reikalavimų pažeidimus, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai EPIS administratoriui.

17.2. EPIS administratorius jam prieinamomis priemonėmis patikrina gautą pranešimą apie pažeidimą ir, faktui pasitvirtinus, užfiksuoja incidentą EPIS elektroninės informacijos saugos incidentų žurnale ir imasi visų įmanomų priemonių pažeidimui užkirsti ar nutraukti.

18. Programinės ir techninės įrangos keitimo ir atnaujinimo tvarka:

18.1. EPIS techninė ir programinė įranga atnaujinama pagal Taisyklių 19 punkte nurodytą EPIS pakeitimų valdymo tvarką.

18.2. EPIS programinės ir techninės įrangos keitimo ir atnaujinimo tvarką su trečia šalimi, kuriai Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme nustatytomis sąlygomis ir tvarka perduotos informacinės sistemos ir (ar) jos infrastruktūros priežiūros funkcijos (toliau – paslaugų teikėjas), atsižvelgiant į konkretų atvejį, derina EPIS administratorius arba ji aprašoma paslaugų, susijusių su EPIS programinės ir techninės įrangos keitimu ir atnaujinimu, teikimo sutartyse ir EPIS priežiūros reglamentuose.

18.3. Perėjimą prie naujos operacinės sistemos versijos inicijuoja EPIS administratorius.

18.4. Apie visus darbus, kurie gali sutrikdyti EPIS veikimą, EPIS administratorius iš anksto privalo informuoti EPIS saugos įgaliotinį ir EPIS naudotojus.

19. EPIS pakeitimų valdymo tvarka:

19.1. EPIS pakeitimų (toliau – pakeitimai) valdymo planavimas apima pakeitimų identifikavimą, suskirstymą į kategorijas pagal pakeitimo tipą (administracinis, organizacinis ar techninis), poveikio vertinimą (svarbumas ir skubumas) ir pakeitimų prioritetų nustatymo procesus.

19.2. EPIS duomenų valdymo įgaliotinis, vadovaudamasis EPIS plėtros planu, kitais EPIS valdytojo planavimo dokumentais:

19.2.1. planuoja pakeitimų valdymą, kas apima pakeitimų identifikavimą, suskirstymą į kategorijas pagal pakeitimo tipą (administracinis, organizacinis ar techninis);

19.2.2. siūlo Tarnybos vadovui ar jo įgaliotam asmeniui pakeitimų poveikio vertinimą (svarbumas ir skubumas) ir pakeitimų prioritetą;

19.2.3. įgyvendina EPIS ar funkciškai savarankiškos jos sudedamosios dalies (toliau – posistemis) plėtrą;

19.2.4. tiesiogiai prižiūri, kaip kuriama ir tvarkoma EPIS, jos posistemiai, diegiama programinė įranga, panaudojamos investicijos;

19.2.5. rengia EPIS biudžeto projektus.

19.3. Pakeitimai identifikuojami pasikeitus su EPIS veikla susijusiems teisės aktams, nustačius naujus EPIS naudotojų, EPIS administratoriaus poreikius, apibendrinus kylančias priežiūros problemas ir kitais gerosios praktikos įvardijamais atvejais.

19.4. Pakeitimus turi teisę inicijuoti EPIS saugos įgaliotinis, EPIS administratorius ar EPIS duomenų valdymo įgaliotinis, o įgyvendinti – EPIS administratorius arba EPIS duomenų valdymo įgaliotinis pagal kompetenciją.

19.5. Visi potencialūs pakeitimai fiksuojami pakeitimų žurnale, įvertinus ir Tarnybos vadovui ar jo įgaliotam asmeniui patvirtinus poveikio vertinimą ir prioritetą.

19.6. EPIS programinės įrangos pakeitimai atliekami tik įvertinus pakeitimų poreikį, pakeitimų apimtį.

19.7. EPIS funkcijų ir galimybių sąrankos aprašai turi būti nuolat atnaujinami ir atspindėti esamą EPIS sąrankos būklę.

19.8. Pakeitimai įgyvendinami Tarnybos vadovo ar jo įgalioto asmens patvirtintu eiliškumu, atsižvelgiant į nustatytą skubumą ar svarbumą.

19.9. Visi diegiami pakeitimai, galintys sutrikdyti ar sustabdyti EPIS darbą, turi būti suderinti su EPIS duomenų valdymo ir saugos įgaliotiniais ir vykdomi tik gavus jų raštišką pritarimą.

19.10. Prieš atlikdamas EPIS pakeitimus, kurių metu gali iškilti grėsmė EPIS duomenų konfidencialumui, vientisumui ar pasiekiamumui, EPIS administratorius privalo įsitikinti, kad planuojami pakeitimai išbandyti testinėje aplinkoje.

19.11. Programinės įrangos testavimas atliekamas naudojant tam skirtą testinę aplinką, kurioje nėra konfidencialių ir asmens duomenų ir kuri atskirta nuo eksploatuojamos EPIS.

19.12. Atlikus planuojamų pakeitimų testavimą, EPIS administratorius gali pradėti įgyvendinti pakeitimus tik suderinęs su EPIS saugos įgaliotiniu.

19.13. Planuodamas pakeitimus, kurių metu galimi EPIS veikimo sutrikimai, EPIS administratorius privalo ne vėliau kaip prieš dvi darbo dienas iki pakeitimų vykdymo pradžios informuoti EPIS naudotojus apie tokių darbų pradžią ir galimus EPIS veikimo sutrikimus.

20. Nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių naudojimo tvarka:

20.1. Nešiojamieji kompiuteriai ir mobilieji įrenginiai turi būti saugomi ir negali būti palikti be priežiūros viešose vietose.

20.2. Visi nešiojamieji kompiuteriai ir kiti mobilieji įrenginiai turi būti apsaugoti saugiais slaptažodžiais, sudėtingumu atitinkančiais EPIS naudotojų administravimo taisyklių reikalavimus.

IV SKYRIUS
REIKALAVIMAI, KELIAMI EPIS FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

21. Reikalavimai EPIS funkcionuoti reikalingoms paslaugoms ir jų teikėjams nustatomi paslaugų teikimo sutartyse.

22. EPIS administratorius atsako už programinių, techninių ir kitų prieigos prie EPIS išteklių priemonių organizavimą, suteikimą ir panaikinimą techninės ir (ar) programinės įrangos priežiūros paslaugos teikėjui.

23. EPIS administratorius suteikia paslaugos teikėjui tik tokią prieigą prie EPIS išteklių, kuri yra būtina norint įvykdyti paslaugų teikimo sutartyje nustatytus įsipareigojimus ir kuri neprieštarauja įstatymų ir kitų teisės aktų reikalavimams.

24. Su paslaugų teikėju turi būti suderinta paslaugos teikimo tvarka, į kurią įtraukti prieigos reikalavimai bei jos suteikimo sąlygos.

25. Pasibaigus sutarties su paslaugos teikėjais galiojimo terminui ar atsiradus paslaugų teikimo sutartyje ar saugos politiką įgyvendinančiuose dokumentuose įvardytų kitų sąlygų, EPIS administratorius nedelsdamas privalo panaikinti suteiktą prieigą.

26. Reikalavimai, keliami paslaugų teikėjų patalpoms, įrangai, EPIS priežiūrai, duomenų perdavimui tinklais ir kitoms paslaugoms, nurodomi paslaugų teikimo sutartyse.

27. Paslaugų teikėjų darbuotojams, atliekantiems administravimo funkcijas, taikomi visi EPIS administratoriui saugos dokumentuose nustatyti reikalavimai.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

28. Asmenys, pažeidę Taisyklių reikalavimus, atsako teisės aktų nustatyta tvarka.

_____

PATVIRTINTA
Lietuvos Respublikos
ryšių reguliavimo tarnybos
direktoriaus
2017 m. gruodžio 22 d.
įsakymu Nr. 1V-1291

LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBOS ELEKTRONINIŲ PASLAUGŲ INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos veiklos tęstinumo valdymo plane (toliau – Planas) nustatomos taisyklės ir procedūros, kurių būtina laikytis atkuriant Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos (toliau – EPIS) veiklą įvykus elektroninės informacijos saugos incidentui (toliau – saugos incidentas).

2. Plane vartojamos sąvokos apibrėžtos 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“.

3. Planas įsigalioja įvykus saugos incidentui.

4. Planas privalomas EPIS valdytojui, tvarkytojui, saugos įgaliotiniui, administratoriui, EPIS naudotojams.

5. EPIS veiklos atkūrimas įvykus saugos incidentui finansuojamas iš Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos nuostatų, patvirtintų Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2016 m. rugsėjo 26 d. įsakymu Nr. 1V-1005 „Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos nuostatų patvirtinimo“, 33 punkte nurodytų šaltinių.

6. EPIS administratorius, EPIS saugos įgaliotinis, prireikus – EPIS naudotojai, nedelsdami šalina saugos incidento padarinius ir įgyvendina kitas EPIS veiklos atkūrimo detaliajame plane (2 priedas) numatytas priemones.

7. Kriterijai, pagal kuriuos nustatoma, kad EPIS veikla atkurta:

7.1. nuolat atnaujinami EPIS duomenys;

7.2. išsaugomi atnaujinti EPIS duomenys;

7.3. EPIS gali naudotis visi EPIS naudotojai.

7.4. iš susijusių registrų ir informacinių sistemų gaunami duomenys yra atnaujinami ir išsaugomi.

8. EPIS veikla laikoma atkurta, jeigu EPIS yra vėl prieinama ne mažiau kaip 90 procentų laiko per parą.

9. EPIS saugos incidento tyrimas atliekamas pagal EPIS saugos incidentų tyrimo tvarkos aprašą (1 priedas).

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

10. Saugos incidentams valdyti ir EPIS veiklai atkurti sudaromos dvi grupės: Veiklos tęstinumo valdymo grupė (toliau – Valdymo grupė) ir Veiklos atkūrimo grupė.

11. Valdymo grupės tikslai – tirti saugos incidentus, ieškoti priemonių ir būdų sukeltiems padariniams ir žalai likviduoti, užtikrinti EPIS veiklos tęstinumą.

12. Valdymo grupės sudėtis:

12.1. grupės vadovas – Lietuvos Respublikos ryšių reguliavimo tarnybos (toliau – Tarnyba) Administracinio departamento Informacinių technologijų skyriaus vedėjas;

12.2. grupės vadovo pavaduotojas – Tarnybos Administracinio departamento Informacinių technologijų skyriaus atstovas;

12.3. grupės nariai – Tarnybos Strategijos departamento Ekonominės analizės skyriaus atstovas, EPIS saugos įgaliotinis.

13. Valdymo grupės funkcijos:

13.1. situacijos analizė, problemų (saugos incidentų) nustatymas;

13.2. sprendimų EPIS veiklos tęstinumo valdymo klausimais priėmimas ir jų vykdymo kontrolė;

13.3. bendravimas su teisėsaugos ir kitomis institucijomis, EPIS naudotojų informavimas;

13.4. finansinių ir kitų išteklių, reikalingų EPIS veiklai atkurti, įvykus saugos incidentui, nustatymas ir naudojimo kontrolė;

13.5. elektroninės informacijos fizinės saugos, įvykus saugos incidentui, užtikrinimas;

13.6. logistikos (žmonių, daiktų, įrangos gabenimas) organizavimas;

13.7. bendravimas su kitų informacinių sistemų veiklos tęstinumo valdymo grupėmis;

13.8. EPIS veiklos atkūrimo priežiūra ir koordinavimas.

14. Veiklos atkūrimo grupės tikslas – likviduoti saugos incidentus.

15. Veiklos atkūrimo grupę sudaro:

15.1. grupės vadovas – Tarnybos Administracinio departamento Informacinių technologijų skyriaus atstovas;

15.2. grupės vadovo pavaduotojas – Tarnybos Administracinio departamento Informacinių technologijų skyriaus atstovas;

15.3. grupės nariai – Tarnybos Strategijos departamento Ekonominės analizės skyriaus atstovas, EPIS administratorius.

16. Veiklos atkūrimo grupės funkcijos:

16.1. tarnybinių stočių veikimo atkūrimo organizavimas;

16.2. kompiuterių tinklo veikimo atkūrimo organizavimas;

16.3. taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

16.4. kompiuterizuotų darbo vietų veikimo atkūrimo ir prijungimo prie kompiuterių tinklo organizavimas;

16.5. EPIS elektroninės informacijos atkūrimo organizavimas.

17. Valdymo ir Veiklos atkūrimo grupių sudėtį įsakymu tvirtina Tarnybos direktorius.

18. Valdymo grupė organizuoja susirinkimą įvykus saugos incidentui.

19. Valdymo grupė, atlikusi situacijos analizę, susisiekia su Veiklos atkūrimo grupe ir informuoja apie esamą padėtį bei priimtus sprendimus dėl EPIS veiklos atkūrimo.

20. Tarpusavyje Valdymo ir Veiklos atkūrimo grupių nariai bendrauja asmeniškai, elektroniniu paštu, telefonu ir kitomis įmanomomis ryšio priemonėmis.

21. EPIS veiklos atkūrimo veiksmai ir už jų vykdymą atsakingi asmenys nurodyti EPIS veiklos tęstinumo detaliajame plane, pateiktame Plano 2 priede.

22. Apie įvykdytus veiklos atkūrimo veiksmus atsakingi asmenys nedelsdami informuoja Veiklos atkūrimo grupės vadovą.

23. Veiklos atkūrimo grupės vadovas nuolat informuoja Valdymo grupės narius apie EPIS veiklos atkūrimo eigą.

24. Atsarginėms patalpoms, naudojamoms EPIS veiklai atkurti saugos incidento metu, esančioms adresu: Sausio 13-osios g. 10, LT-04347 Vilnius, keliami tokie reikalavimai:

24.1. Patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų.

24.2. Patalpose turi būti įrengta langų ir durų fizinė apsauga.

24.3. Patalpos privalo atitikti priešgaisrinės saugos reikalavimus, jose turi būti gaisro gesinimo priemonės.

24.4. Ryšių kabeliai turi būti apsaugoti nuo neteisėto prisijungimo prie jų ir pažeidimo.

24.5. Privalo būti įgyvendintos gamintojo nustatytos techninės įrangos darbo sąlygos.

24.6. Patalpose turi būti patikimas elektros energijos tiekimas per nenutrūkstamo maitinimo šaltinius.

24.7. Patalpose būtina interneto ryšio prieiga.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

25. Informacinių technologijų įrangos sąrašai, šios įrangos parametrai ir už jos priežiūrą atsakingi asmenys nurodyti elektroniniame žurnale, kurį tvarko EPIS administratorius. Elektroninio žurnalo kopijos saugomos archyve. Nesant EPIS administratoriaus, jį gali pavaduoti kitas darbuotojas, atitinkantis Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos saugos nuostatų, patvirtintų Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2016 m. rugsėjo 26 d. įsakymu Nr. 1V-1006 „Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos saugos nuostatų patvirtinimo“, 30 punkte EPIS administratoriui nustatytus reikalavimus.

26. Tarnybos pastato, kuriame yra tarnybinė stotis, aukšto planas saugomas Tarnybos Administracinio departamento Turto valdymo ir logistikos skyriuje.

27. Patalpose esančios įrangos ir komunikacijų brėžiniai saugomi Tarnybos Administracinio departamento Informacinių technologijų skyriuje.

28. Duomenų teikimo ir pagrindinės kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąrašai saugomi Tarnybos Administracinio departamento Informacinių technologijų skyriuje.

29. Programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis žurnalas, kuriame nurodoma programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos, saugomas Tarnybos Administracinio departamento Informacinių technologijų skyriuje.

30. Veiklos valdymo grupės ir Veiklos atkūrimo grupės narių telefonų numeriai skelbiami Tarnybos interneto svetainėje ir saugomi EPIS saugos įgaliotinio.

IV SKYRIUS
PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

31. Plano veiksmingumas turi būti išbandytas per šešis mėnesius nuo jo patvirtinimo dienos. Plano veiksmingumas turi būti išbandomas ne rečiau kaip kartą per metus, modeliuojant saugos incidentą.

32. Išbandymo rezultatai pateikiami plano veiksmingumo išbandymo ataskaitoje (3 priedas), kurią parengia EPIS saugos įgaliotinis kartu su EPIS administratoriumi. Už plano veiksmingumo išbandymo ataskaitos pateikimą Tarnybos direktoriui ar jo įgaliotam asmeniui atsakingas EPIS saugos įgaliotinis.

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

_____

Lietuvos Respublikos ryšių reguliavimo
tarnybos elektroninių paslaugų
informacinės sistemos veiklos tęstinumo
valdymo plano
1 priedas

EPIS SAUGOS INCIDENTŲ TYRIMO TVARKOS APRAŠAS

1. EPIS naudotojai, pastebėję saugos dokumentų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti EPIS administratoriui.

2. EPIS administratorius nedelsdamas turi imtis veiksmų, reikalingų saugos incidentui stabdyti, padariniams likviduoti, ir apie tai pranešti EPIS saugos įgaliotiniui, kuris, įvertinęs incidento reikšmingumą, informuoja Valdymo grupės vadovą.

3. EPIS saugos įgaliotinis su EPIS administratoriumi nagrinėja saugos incidentą, priskiria jį tam tikrai klasei ir priima sprendimą dėl saugos incidento svarbos lygio.

4. EPIS administratorius, suderinęs su EPIS saugos įgaliotiniu, atlieka neatidėliotinus EPIS administravimo veiksmus, skirtus saugos incidento plėtrai sustabdyti ir tyrimui būtinai informacijai surinkti.

5. EPIS administratorius surenka visą su saugos incidentu susijusią informaciją ir įvykį fiksuoja EPIS saugos incidentų žurnale (priedas), nurodydamas incidento vietą, laiką, pobūdį, sistemos atkuriamuosius darbus ir kitą su saugos incidentu susijusią informaciją, informuoja apie saugos incidentą pranešusį asmenį apie pašalintus saugos incidento sukeltus nesklandumus.

6. Incidentui paveikus kitas, ne Tarnybos valdomas informacines sistemas, EPIS administratorius informuoja saugos incidento poveikį patyrusius ar galinčius patirti paslaugų teikėjus ir (ar) kitas institucijas, atsižvelgia į jų rekomendacijas ir vykdo jų nurodymus.

7. Valdymo grupės vadovas, atsižvelgdamas į saugos incidento pobūdį, gali inicijuoti jo išsamų tyrimą.

8. Nusprendęs pradėti saugos incidento tyrimą, Valdymo grupės vadovas teikia Tarnybos vadovui siūlymą sudaryti atskirą tyrimo komisiją, kuri per penkiolika darbo dienų turi:

8.1. ištirti saugos incidento atsiradimo priežastis;

8.2. nustatyti asmenis, dėl kurių veiksmų ir (ar) neveikimo įvyko saugos incidentas;

8.3. nustatyti saugos incidento pasekmes ar dėl jo atsiradusią žalą;

8.4. parengti ir pateikti Valdymo grupės vadovui tyrimo išvadas.

9. Valdymo grupės vadovas, atsižvelgdamas į tyrimo komisijos pateiktas išvadas, turi teisę teikti Tarnybos vadovui siūlymus dėl atsakomybės taikymo teisės aktų nustatyta tvarka.

_____

Elektroninių paslaugų informacinės sistemos
elektroninės informacijos saugos incidentų
tyrimo tvarkos aprašo
priedas

(EPIS saugos incidentų apskaitos žurnalo forma)

LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBOS ELEKTRONINIŲ PASLAUGŲ INFORMACINĖS SISTEMOS ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTŲ ŽURNALAS

Eil. Nr.	**Elektroninės informacijos saugos incidentas**						
	Informacinės sistemos naudotojo padalinio pavadinimas	**Požymio kodas***	**Elektroninės informacijos saugos incidento aprašymas**	**Pradžia (metai, mėnuo, diena, valanda)**	**Pabaiga (metai, mėnuo, diena, valanda)**	**Elektroninės informacijos saugos incidentą pašalinusio (-ių) darbuotojo (-ų) v. pavardė**	**Saugos įgaliotinis (v. pavardė, parašas)**
1	2	3	4	5	6	7	8

* Elektroninės informacijos saugos incidento požymių kodai:
1 – gamtos reiškiniai; 2 – gaisras; 3 – elektros energijos tiekimo sutrikimai; 4 – vandentiekio ir šildymo sistemų sutrikimai; 5 – ryšio sutrikimai; 6 – įsilaužimas į vidinį kompiuterių tinklą; 7 – pagrindinių tarnybinių stočių sugadinimas ir (ar) praradimas; 8 – vagystė iš duomenų bazės ar jos fizinis sunaikinimas; 9 – programinės įrangos sugadinimas, praradimas; 10 – pavojingas (įtartinas) radinys; 11 – įvykis, susijęs su teroristine veikla; 12 – dokumentų praradimas; 13 – dalinis informacinės sistemos sutrikimas dėl neaiškių priežasčių.

Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos veiklos tęstinumo valdymo plano
2 priedas

EPIS VEIKLOS TĘSTINUMO DETALUSIS PLANAS

Eil. Nr.	Elektroninės informacijos saugos incidentas	Pirmaeiliai veiksmai	Pasekmių likvidavimo veiksmai	Terminai	Atsakingi vykdytojai
1	2	3	4	5	6
1.	Gamtos reiškiniai (potvynis, uraganas, ir kiti)	1.1. Elektroninės informacijos saugos incidento padarinių įvertinimas, priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas ir įgyvendinimas	1.1.1. Elektroninės informacijos saugos incidento metu padarytos žalos įvertinimas	Per 15 min. nuo incidento nustatymo	Valdymo grupės vadovas
			1.1.2. Priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas	Per 30 min. nuo incidento nustatymo	Valdymo grupės vadovas
			1.1.3. Darbuotojų informavimas, padarytą žalą likviduojančių darbuotojų instruktavimas	Nedelsiant	EPIS saugos įgaliotinis
			1.1.4. Elektroninės informacijos saugos incidento metu padarytos žalos likvidavimas, pirmosios pagalbos suteikimas nukentėjusiems darbuotojams	Nedelsiant	EPIS administratorius
2.	Gaisras	2.1. Priešgaisrinės gelbėjimo tarnybos informavimas	2.1.1. Įvykio vietos lokalizavimas, jei yra rekomendacija iš Priešgaisrinės gelbėjimo tarnybos	Nedelsiant	EPIS saugos įgaliotinis

		2.2. Gaisro gesinimas ankstyvoje stadijoje, jei yra rekomendacija dirbti pavojaus zonoje	2.2.1. Galimybių evakuoti darbuotojus įvertinimas, jei Priešgaisrinė gelbėjimo tarnyba rekomenduoja	Nedelsiant	Valdymo grupės vadovas EPIS saugos įgaliotinis
		2.3. Darbas pavojaus zonoje: komunikacijų, sukeliančių pavojų, išjungimas	2.3.1. Darbuotojų informavimas apie evakavimą, jei yra rekomendacija	Nedelsiant	EPIS saugos įgaliotinis
		2.4. Sutrikimų pašalinimas	2.4.1. Darbuotojų informavimas apie saugų darbą pavojaus zonoje	Nedelsiant	EPIS saugos įgaliotinis
			2.4.2 Elektroninės informacijos saugos incidento metu padarytos žalos įvertinimas	Per 1 val. nuo incidento nustatymo	Valdymo grupės vadovas
			2.4.3. Padarytą žalą likviduojančių darbuotojų instruktavimas	Nedelsiant	EPIS saugos įgaliotinis
			2.4.4. Elektroninės informacijos saugos incidento metu padarytos žalos likvidavimas	Priklausomai nuo atkūrimo darbų apimties	EPIS administratorius
3.	Elektros energijos tiekimo sutrikimai	3.1. Elektros tiekimo sutrikimo priežasčių nustatymas	3.1.1. Rekomendacijų iš elektros energijos tiekimo tarnybos gavimas	Per 1 val. nuo incidento nustatymo	Valdymo grupės vadovas
		3.2. Tarnybinių stočių, kitos techninės įrangos maitinimo išjungimas	3.2.1. Padarytos žalos įvertinimas	Per 1,5 val. nuo incidento nustatymo	Valdymo grupės vadovas
		3.3. Kreipimasis į elektros energijos tiekimo tarnybą dėl pavojaus trukmės ir sutrikimo pašalinimo galimybių	3.3.1. Žalą likviduojančių darbuotojų instruktavimas	Nedelsiant	EPIS saugos įgaliotinis
		3.4. Sutrikimų pašalinimas	3.4.1. Padarytos žalos likvidavimas	Priklausomai nuo atkūrimo darbų apimties	EPIS saugos įgaliotinis, EPIS

					administratorius, Valdymo grupės vadovas
4.	Vandentiekio ir šildymo sistemų sutrikimai	4.1. Vandentiekio ar šildymo paslaugų teikėjų informavimas	4.1.1. Paslaugų teikėjų rekomendacijų gavimas	Per 1 val. nuo incidento nustatymo	Veiklos grupės vadovas
			4.1.2. Darbuotojų informavimas apie rekomendacijas	Iš karto po rekomendacijų gavimo	EPIS saugos įgaliotinis
		4.2. Sutrikimo šalinimo prognozės skelbimas	4.2.1. Padarytos žalos įvertinimas	Per 1 val. nuo incidento nustatymo	Veiklos grupės vadovas
			4.2.2. Padarytos žalos likvidavimas	Priklausomai nuo atkūrimo darbų apimties	Veiklos grupės vadovas
5.	Elektroninių ryšių tinklo sutrikimas	5.1. Ryšio sutrikimo priežasčių nustatymas	5.1.1. Ryšio paslaugos teikėjo rekomendacijų gavimas	Per 1 val. nuo incidento nustatymo	EPIS administratorius
		5.2. Ryšio tarnybų informavimas, sutrikimo trukmės ir šalinimo prognozavimas	5.2.1. Sutrikimo likvidavimas	Priklausomai nuo atkūrimo darbų apimties	EPIS administratorius
6.	Įsilaužimas į vidinį kompiuterių tinklą	6.1. Pranešti teisėsaugos institucijai apie įvykį	6.1.1. Teisėsaugos institucijos nurodymų vykdymas	Nedelsiant	EPIS saugos įgaliotinis
		6.2. Priemonių plano sudarymas ir įgyvendinimas	6.2.1. Elektroninės informacijos saugos incidento pasekmių likvidavimas	Nedelsiant	EPIS administratorius
7.	Pagrindinių tarnybinių stočių sugadinimas ir (ar) praradimas	7.1. Pranešti teisėsaugos institucijai apie įvykį	7.1.1. Teisėsaugos institucijos nurodymų vykdymas	Nedelsiant	Valdymo grupės vadovas
		7.2. Priemonių plano sudarymas ir įgyvendinimas	7.2.1. Padarytą žalą likviduojančių darbuotojų instruktavimas	Nedelsiant	EPIS saugos įgaliotinis

			7.2.2. Elektroninės informacijos saugos incidento pasekmių likvidavimas	Priklausomai nuo atkūrimo darbų apimties	EPIS administratorius
			7.2.3. Padarytos žalos įvertinimas	Per 1 val. nuo incidento nustatymo	Valdymo grupės vadovas
			7.2.4. Žalos likvidavimas	Priklausomai nuo atkūrimo darbų apimties	Valdymo grupės vadovas
8.	Vagystė iš duomenų bazės ar jos fizinis sunaikinimas	8.1. Pranešti teisėsaugos institucijai apie įvykį	8.1.1. Teisėsaugos institucijos nurodymų vykdymas	Nedelsiant	Valdymo grupės vadovas
		8.2. Priemonių plano sudarymas ir įgyvendinimas	8.2.1. Padarytos žalos įvertinimas	Per 1 val. nuo incidento nustatymo	Valdymo grupės vadovas
			8.2.2. Duomenų atkūrimas iš atsarginių kopijų	Per 8 val.	EPIS administratorius
9.	Programinės įrangos sugadinimas, praradimas	9.1. Pranešti teisėsaugos institucijai apie įvykį	9.1.1. Teisėsaugos institucijos nurodymų vykdymas, priemonių plano sudarymas ir įgyvendinimas	Per 1 val. nuo incidento nustatymo	Valdymo grupės vadovas
		9.2. Programinės įrangos kopijų periodinis gaminimas	9.2.1. Elektroninės informacijos saugos incidento metu padarytos žalos įvertinimas	Per 1 val. nuo incidento nustatymo	Valdymo grupės vadovas
			9.2.2. Žalą likviduojančių darbuotojų instruktavimas	Nedelsiant	EPIS saugos įgaliotinis
			9.2.3. Padarytos žalos likvidavimas	Priklausomai nuo atkūrimo darbų apimties	EPIS administratorius
10.	Pavojingas (įtartinas) radinys	10.1. Pranešti teisėsaugos institucijai apie įvykį	10.1.1. Teisėsaugos institucijos nurodymų vykdymas	Nedelsiant	Valdymo grupės vadovas

11.	Įvykis, susijęs su teroristine veikla	11.1. Pranešti teisėsaugos institucijai apie įvykį	11.1.1. Teisėsaugos institucijos nurodymų vykdymas	Nedelsiant	Valdymo grupės vadovas
		11.2. Darbuotojų evakavimas, jei yra rekomendacija	11.2.1. Darbuotojų informavimas apie nurodymų vykdymą	Nedelsiant	EPIS saugos įgaliotinis
12.	Dokumentų praradimas	12.1. Vadovybės informavimas	12.1.1. Prarastų dokumentų atkūrimas	Per 8 val. nuo incidento nustatymo	EPIS saugos įgaliotinis
13.	Dalinis informacinės sistemos veiklos sutrikimas dėl nenustatytų priežasčių	13.1. Informuojami atsakingi darbuotojai. Organizuojamas techninių specialistų pasitarimas problemai nustatyti	13.1.1. Padarytos žalos įvertinimas	Nedelsiant	EPIS saugos įgaliotinis
		13.2. Lokalizuojama problema	13.2.1. Padarytą žalą likviduojančių darbuotojų instruktavimas	Nedelsiant	EPIS administratorius
		13.3. Problema šalinama	13.3.1. Elektroninės informacijos saugos incidento pasekmių likvidavimas	Nedelsiant	Valdymo grupės vadovas

Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos veiklos tęstinumo valdymo plano
3 priedas

(Plano veiksmingumo išbandymo ataskaitos forma)

LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBOS ELEKTRONINIŲ PASLAUGŲ INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANO VEIKSMINGUMO IŠBANDYMO ATASKAITA

_____ Nr.
(data)

1. Plano išbandymo data:
2. Bandyme dalyvavo:

_____
(pareigos, vardas, pavardė)

3. Elektroninės informacijos saugos incidento scenarijus:

_____

4. Funkcijos ir posistemiai, kuriuos paveikė elektroninės informacijos saugos incidentas:

_____

5. Elektroninės informacijos saugos incidento šalinimo eiga:

_____

6. Rasti trūkumai:

_____

7. Pasiūlymai keisti arba papildyti planą:

_____

EPIS saugos įgaliotinis:

_____	_____	_____
(pareigos)	(parašas)	(vardas ir pavardė)

EPIS administratorius:

_____	_____	_____
(pareigos)	(parašas)	(vardas ir pavardė)

PATVIRTINTA
Lietuvos Respublikos ryšių
reguliavimo tarnybos direktoriaus 2017
m. gruodžio 22 d. įsakymu Nr. 1V-1291

LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBOS ELEKTRONINIŲ PASLAUGŲ INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos naudotojų administravimo taisyklės (toliau – Taisyklės) reglamentuoja Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos (toliau – EPIS) naudotojų ir administratorių įgaliojimus, teises, pareigas, jų supažindinimo su saugos dokumentais tvarką ir saugaus EPIS tvarkomų duomenų teikimo EPIS naudotojams kontrolės tvarką.

2. Taisyklėse vartojamos sąvokos apibrėžtos 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“.

3. Taisyklės taikomos visiems EPIS naudotojams ir EPIS administratoriams (toliau visi kartu – naudotojai).

4. Naudotojai turi turėti tik tiek prieigos prie EPIS duomenų teisių, kiek tai būtina jų tiesioginei veiklai vykdyti.

5. Prieiga prie EPIS naudotojams suteikiama vadovaujantis principu „*būtina žinoti*“.

II SKYRIUS
EPIS NAUDOTOJŲ IR EPIS ADMINISTRATORIŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

6. Naudotojai turi teisę tvarkyti EPIS elektroninę informaciją tik atlikdami savo tiesiogines funkcijas.

7. Naudotojams draudžiama savavališkai tvarkyti EPIS elektroninę informaciją.

8. EPIS administratoriams suteikiama teisė:

8.1. paskirstyti ir tvarkyti fizinę duomenų saugojimo erdvę;

8.2. organizuoti ir atlikti duomenų bazės atkūrimo darbus;

8.3. diegti naujas duomenų bazės valdymo sistemų versijas;

8.4. stebėti EPIS prieinamumą;

8.5. atlikti duomenų kopijavimo darbus;

8.6. prižiūrėti keitimosi duomenimis infrastruktūrą;

8.7. atlikti ypatingos svarbos duomenų pakeitimus;

8.8. administruoti EPIS tarnybines stotis;

8.9. administruoti EPIS naudotojų – Lietuvos Respublikos ryšių reguliavimo tarnybos (toliau – Tarnyba) valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartį, (toliau – darbuotojai) − kompiuterizuotas darbo vietas.

9. Naudotojai vykdo EPIS saugos įgaliotinio nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu.

10. EPIS naudotojams suteikiama teisė:

10.1. įvesti, keisti, atnaujinti, naikinti EPIS duomenis, susijusius su jų atliekamomis funkcijomis;

10.2. atlikti duomenų paiešką ir peržiūrą.

11. Naudotojas, jungdamasis prie EPIS, privalo atlikti tapatumo nustatymo procedūrą, autentifikuodamas savo tapatybę per Valstybės informacinių išteklių sąveikumo platformą (toliau – VIISP).

12. Naudotojai privalo laikytis Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos saugos nuostatuose, patvirtintuose Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2016 m. rugsėjo 26 d. įsakymu Nr. 1V-1006 „Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos saugos nuostatų patvirtinimo“, (toliau – EPIS saugos nuostatai), kituose EPIS saugos politiką įgyvendinančiuose dokumentuose (toliau – saugos dokumentai) ir kituose teisės aktuose nustatytų reikalavimų.

13. Naudotojai privalo užtikrinti EPIS duomenų saugumą.

III SKYRIUS
NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS TVARKA

14. Naudotojai su saugos dokumentais supažindinami pasirašytinai.

15. Naudotojus su saugos dokumentais supažindina EPIS saugos įgaliotinis. Naudotojų susipažinimo su duomenų saugos dokumentais sąrašus saugo EPIS saugos įgaliotinis.

16. Naudotojai pakartotinai su saugos dokumentais supažindinami tik šiems dokumentams iš esmės pasikeitus.

IV SKYRIUS
SAUGAUS DUOMENŲ TEIKIMO NAUDOTOJAMS KONTROLĖS TVARKA

17. Naudotojų įregistravimo ir išregistravimo tvarka:

17.1. EPIS naudotojus įregistruoja ir išregistruoja EPIS administratorius.

17.2. EPIS naudotojai įregistruojami ir išregistruojami remiantis Tarnybos atitinkamo departamento vadovo tarnybiniu pranešimu.

17.3. EPIS administratorius, jungdamasis prie duomenų bazių, papildomai tapatybę patvirtina naudodamas naudotojo vardą ir slaptažodį. EPIS administratoriui suteikiamas nesikartojantis naudotojo vardas ir laikinas slaptažodis. EPIS administratoriui suteiktas naudotojo vardas nekeičiamas ir negali būti suteiktas kitam EPIS naudotojui.

17.4. Naudotojai turi būti autentifikuojami VIISP autentifikavimo priemonėmis arba naudoti suteiktą naudotojo vardą. Naudoti svetimą naudotojo vardą griežtai draudžiama.

18. Reikalavimai slaptažodžių sudarymui, galiojimo trukmei, keitimui ir saugojimui:

18.1. Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu ar užšifruojami nepatikimais algoritmais; saugos įgaliotinio sprendimu tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jei:

18.1.1. EPIS naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio;

18.1.2. nėra techninių galimybių EPIS naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu.

18.2. Suteiktas laikinas slaptažodis turi būti pakeistas pirmojo prisijungimo prie EPIS metu.

18.3. EPIS naudotojo slaptažodį turi sudaryti ne mažiau kaip 8 simboliai, EPIS administratoriaus – ne mažiau kaip 12 simbolių.

18.4. Slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių.

18.5. Slaptažodžiui sudaryti patartina nenaudoti asmeninės informacijos (pvz., savo ar vaiko gimimo datos, gyvenamosios vietos adreso sudėtinių dalių, namo, buto numerio, vaikų vardų ir t. t.), nesudaryti iš žodynuose pateikiamų žodžių, nenaudoti iš eilės einančių skaičių ar raidžių.

18.6. EPIS naudotojo slaptažodis turi būti keičiamas ne rečiau kaip kas 90 dienų, EPIS administratoriaus – ne rečiau kaip kas 60 dienų.

18.7. Draudžiama naudoti tą patį slaptažodį darbo ir nedarbinei veiklai.

18.8. Slaptažodis turi būti įsimenamas, draudžiama slaptažodį užsirašyti ar atskleisti kitam asmeniui.

18.9. Kilus įtarimui, kad slaptažodis galėjo būti atskleistas, EPIS naudotojas turi nedelsdamas slaptažodį pakeisti.

18.10. Pasirinkdamas ar keisdamas slaptažodį, EPIS naudotojas turi bent kartą slaptažodį pakartoti.

18.11. Keičiant EPIS naudotojo slaptažodį, EPIS neturi leisti sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių, EPIS administratoriaus – iš buvusių 3 paskutinių slaptažodžių.

18.12. Slaptažodžiai turi būti saugomi naudojant maišos funkcijas.

18.13. EPIS dalys, atliekančios nuotolinio prisijungimo autentikavimą, turi neleisti automatiškai išsaugoti slaptažodžius.

19. Didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius – 5 kartai; neteisingai įvedus slaptažodį didžiausią leistiną mėginimų skaičių, EPIS užsirakina ir neleidžia naudotojui identifikuotis EPIS 15 minučių.

20. Naudotojams prieigos teisės dirbti su EPIS gali būti suteiktos tik pasirašius pasižadėjimą saugoti tvarkomų duomenų paslaptį, laikytis duomenų saugos reikalavimų ir pasirašytinai susipažinus su saugos dokumentais.

21. EPIS naudotojų teisės dirbti su EPIS elektronine informacija ribojimas ir naikinimas:

21.1. Iš darbo atleidžiamo EPIS naudotojo padalinio vadovas arba jo įgaliotas asmuo elektroniniu laišku informuoja EPIS administratorių apie prieigos teisių dirbti su EPIS elektronine informacija panaikinimą ne vėliau kaip paskutinę EPIS naudotojo darbo Tarnyboje dieną. Atleistų Tarnybos darbuotojų EPIS naudotojo registracijos duomenys nedelsiant blokuojami.

21.2. Keičiantis darbuotojo pareiginėms funkcijoms, turi būti peržiūrimos jo prieigos prie EPIS teisės.

22. Nuotoliniam prisijungimui prie EPIS taikomi reikalavimai:

22.1. Visi nuotoliniai prisijungimai prie EPIS turi būti šifruojami ir fiksuojami kontrolės žurnale.

22.2. Leidimą EPIS naudotojams prisijungti nuotoliniu būdu prie EPIS duoda Tarnybos direktorius ar jo įgaliotas asmuo.

22.3. EPIS naudotojams nuotolinę prieigą prie EPIS suteikia EPIS administratorius, gavęs Tarnybos direktoriaus ar jo įgalioto asmens raštišką leidimą.

_____