Suvestinė redakcija nuo 2023-07-04 iki 2023-12-31

Įsakymas paskelbtas: TAR 2019-07-03, i. k. 2019-10972

LIETUVOS RESPUBLIKOS KRAŠTO APSAUGOS MINISTRAS

ĮSAKYMAS DĖL SAUGIOJO VALSTYBINIO DUOMENŲ PERDAVIMO TINKLO VEIKLĄ UŽTIKRINANČIŲ DOKUMENTŲ PATVIRTINIMO

2019 m. liepos 2 d. Nr. V-583
Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 43^2 straipsnio 4 ir 8 dalimis, Lietuvos Respublikos Vyriausybės 2018 m. sausio 3 d. nutarimo Nr. 27 „Dėl Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo įgyvendinimo Saugiojo valstybinio duomenų perdavimo tinklo valdymo srityje“ 2.1 papunkčiu, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Kibernetinio saugumo įstatymo įgyvendinimo“, 5.3 papunkčiu:

Preambulės pakeitimai:
Nr. V-831, 2021-10-26, paskelbta TAR 2021-10-26, i. k. 2021-22243
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

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

1.1. Prisijungimo prie Saugiojo valstybinio duomenų perdavimo tinklo, atsijungimo nuo jo ir elektroninių ryšių paslaugų teikimo šiuo tinklu tvarkos aprašą;

1.2. Specialiųjų organizacinių ir techninių reikalavimų, taikomų Saugiajam valstybiniam duomenų perdavimo tinklui, juo teikiamoms paslaugoms bei prekių ir paslaugų Saugiajam valstybiniam duomenų perdavimo tinklui teikėjams, aprašą;

1.3. Saugiojo tinklo naudotojų administravimo taisykles.

Papildyta papunkčiu:
Nr. V-207, 2021-03-25, paskelbta TAR 2022-12-05, i. k. 2022-24736

1.4. Saugiojo tinklo veiklos tęstinumo planą;

Papildyta papunkčiu:
Nr. V-286, 2021-04-22, paskelbta TAR 2021-04-22, i. k. 2021-08376

1.5. Saugiojo tinklo incidentų, pokyčių ir problemų valdymo tvarkos aprašą.

Papildyta papunkčiu:
Nr. V-338, 2021-05-11, paskelbta TAR 2021-05-11, i. k. 2021-10495

2. N u s t a t a u, kad Saugiojo valstybinio duomenų perdavimo tinklo naudotojai, įtraukti į Saugiojo valstybinio duomenų perdavimo tinklo naudotojų sąrašą, patvirtintą Lietuvos Respublikos Vyriausybės 2018 m. sausio 3 d. nutarimu Nr. 27 „Dėl Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo įgyvendinimo Saugiojo valstybinio duomenų perdavimo tinklo valdymo srityje“, kurie iki 2019 m. birželio 30 d. naudojosi šio tinklo paslaugomis, iki 2022 m. sausio 1 d. turi įvykdyti šio įsakymo 1 punktu patvirtintų teisės aktų reikalavimus.

Punkto pakeitimai:
Nr. V-393, 2020-05-19, paskelbta TAR 2020-05-20, i. k. 2020-10651

Vidaus reikalų ministras,
pavaduojantis krašto apsaugos ministrą Eimutis Misiūnas

PATVIRTINTA
Lietuvos Respublikos
krašto apsaugos ministro
2019 m. liepos 2 d.
įsakymu Nr. V-583
(Lietuvos Respublikos
krašto apsaugos ministro
2022 m. kovo 28 d.
įsakymo Nr. V-268
redakcija)

PRISIJUNGIMO PRIE SAUGIOJO VALSTYBINIO DUOMENŲ PERDAVIMO TINKLO, ATSIJUNGIMO NUO JO IR ELEKTRONINIŲ RYŠIŲ PASLAUGŲ TEIKIMO ŠIUO TINKLU TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Prisijungimo prie Saugiojo valstybinio duomenų perdavimo tinklo, atsijungimo nuo jo ir elektroninių ryšių paslaugų teikimo šiuo tinklu tvarkos aprašas (toliau – Tvarkos aprašas) nustato prisijungimo prie Saugiojo valstybinio duomenų perdavimo tinklo (toliau – Saugusis tinklas) ir atsijungimo nuo jo sąlygas, Saugiuoju tinklu teikiamų elektroninių ryšių paslaugų (toliau – paslaugos) teikimo sąlygas, taisykles, standartinių paslaugų kiekybinius ir kokybinius rodiklius.

2. Tvarkos aprašas privalomas visoms valstybės ir savivaldybių institucijoms ir įstaigoms, valstybės įmonėms ir viešosioms įstaigoms, įtrauktoms į Lietuvos Respublikos Vyriausybės tvirtinamą Saugiojo tinklo naudotojų (toliau – naudotojas) sąrašą, ir Saugiojo tinklo tvarkytojui.

3. Tvarkos apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo, Lietuvos Respublikos kibernetinio saugumo bei Lietuvos Respublikos elektroninių ryšių įstatymuose bei šiuos įstatymus įgyvendinančiuose teisės aktuose.

4. Saugiuoju tinklu teikiamų standartinių elektroninių ryšių paslaugų (toliau – standartinės paslaugos) kiekybiniai ir kokybiniai rodikliai nurodomi Tvarkos aprašo 1 priede.

II SKYRIUS
PRISIJUNGIMO PRIE SAUGIOJO TINKLO IR ATSIJUNGIMO NUO JO SĄLYGOS

PIRMASIS SKIRSNIS
PRISIJUNGIMAS PRIE SAUGIOJO TINKLO

5. Naudotojas, norėdamas prisijungti prie Saugiojo tinklo, privalo:

5.1. paslaugų teikimo vietoje ar vietose skirti Saugiojo tinklo įrangai patalpą (ar jos dalį), kurioje:

5.1.1. drėgmė, ventiliacija ir temperatūra atitinka toliau pateiktus dydžius ir yra aplinkos sąlygų užtikrinimo sistemos:

5.1.1.1. oro temperatūra 10–30 °C;

5.1.1.2. oro drėgnumas 10–80 proc., nėra drėgmės kondensavimosi sąlygų;

5.1.2. užtikrinami pagrindiniai elektros maitinimo reikalavimai:

5.1.2.1. įtampa 230 V, 50 Hz;

5.1.2.2. galingumas 0,7 kW;

5.1.2.3. įrengtas įžeminimas, įtampos filtras arba kitas įrenginys, užtikrinantis apsaugą nuo įtampos svyravimų ir apsaugą nuo žaibo iškrovos;

5.1.2.4. jei naudotojo elektros sistemos nepertraukiamas veikimas užtikrinamas pasitelkiant nepertraukiamo maitinimo šaltinius ir (ar) dyzelinį generatorių, turi būti užtikrinama, kad Saugiojo tinklo įrangos elektros linija taip pat būtų prijungta prie nepertraukiamą maitinimą užtikrinančių sistemų;

5.1.3. įrengtos priešgaisrinės saugos priemonės Lietuvos Respublikos priešgaisrinės saugos įstatymo ir jį įgyvendinančių teisės aktų nustatyta tvarka;

5.1.4. patekimas į patalpą, kurioje yra Saugiojo tinklo įranga, kontroliuojamas mechaniniais užraktais arba elektronine įeigos kontrolės sistema;

5.2. užtikrinti galimybę Saugiojo tinklo tvarkytojui įrengti vietinę prieigos dalį nuo Saugiojo tinklo įvado į pastatą (optinių ar varinių gijų kabeliu) iki patalpų, kuriose įrengta Saugiojo tinklo įranga, ir iki jose esančios Saugiojo tinklo įrangos;

5.3. užtikrinti galimybę susipažinti su naudotojo saugos politiką reglamentuojančiais dokumentais, parengtais pagal Bendrųjų elektroninės informacijos saugos reikalavimų aprašą, Saugos dokumentų turinio gairių aprašą ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašą, patvirtintus 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“, ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašą, patvirtintą Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, bei šiuose dokumentuose keliamų reikalavimų įgyvendinimu, jei šių dokumentų rengimas pagal minėtus teisės aktus naudotojui yra privalomas;

5.4. užtikrinti *Ethernet 10/100/1000 base T* prievadą naudotojo vietinio kompiuterių tinklo įrenginyje (komutatoriuje ar maršruto parinktuve), per kurį naudotojo vietinis kompiuterių tinklas bus prijungtas prie Saugiojo tinklo. Jei šis įrenginys bus nutolęs daugiau kaip 10 m nuo Saugiojo tinklo įrangos įrengimo vietos, naudotojas turi įrengti ne žemesnės kaip 5 kategorijos (CAT5e) *Ethernet* arba optinį kabelį nuo Saugiojo tinklo įrangos prievado iki naudotojo kompiuterių tinklo maršruto parinktuvo ar komutatoriaus;

5.5. patvirtinti vidinius teisės aktus, kuriuose:

5.5.1. numatoma asmenų patekimo į patalpas, kuriose yra Saugiojo tinklo įranga, kontrolė ir apribojimai;

5.5.2. numatomas asmenų, turinčių teisę patekti į patalpas, kuriose yra Saugiojo tinklo įranga, sąrašas, taip pat į sąrašą neįtrauktų asmenų patekimo į patalpas tvarka ir sąlygos;

5.6. paskirti vieną ar kelis asmenis, įgaliotus atstovauti naudotojui prisijungimo prie Saugiojo tinklo administravimo, saugos organizavimo ir įgyvendinimo klausimais visą prisijungimo

laiką, Saugiojo tinklo tvarkytojui teikti šio asmens (asmenų) kontaktinius duomenis (vardą, pavardę, telefono numerį, elektroninio pašto adresą), o pasikeitus įgaliotiems asmenims ar kontaktinei informacijai atnaujintą informaciją ne vėliau kaip per 5 darbo dienas nuo pasikeitimų dienos pateikti Saugiojo tinklo tvarkytojui.

6. Saugiojo tinklo tvarkytojas į Saugiojo tinklo naudotojų sąrašą naujai įtrauktą naudotoją per 10 darbo dienų informuoja apie Saugiuoju tinklu teikiamas paslaugas ir naudotojui taikomus prisijungimo prie Saugiojo tinklo reikalavimus, nurodytus Tvarkos aprašo 5 punkte.

7. Naudotojas ne vėliau kaip per 20 darbo dienų nuo 6 punkte nurodytos informacijos gavimo iš Saugiojo tinklo tvarkytojo dienos privalo Saugiojo tinklo tvarkytojui pateikti:

7.1. užpildytą Paslaugų užsakymo paraišką (Tvarkos aprašo 2 priedas);

7.2. informaciją apie atitiktį Tvarkos aprašo 5 punkte nustatytiems reikalavimams. Tvarkos aprašo 1 priedo 5 punkte nurodytos paslaugos teikimo vietai atitikties Tvarkos aprašo 5 punktui reikalavimai netaikomi ir informacijos teikti nereikia.

8. Jei naudotojas neatitinka Tvarkos aprašo 5 punkte nurodytų reikalavimų, per 7 punkte nurodytą terminą apie tai informuoja Saugiojo tinklo tvarkytoją, neteikdamas 7 punkte nurodytos informacijos, ir ne vėliau kaip per 3 mėnesius tuos reikalavimus įgyvendina. Įgyvendinęs reikalavimus, pateikia Saugiojo tinklo tvarkytojui 7 punkte nurodytą informaciją.

9. Jei Saugiojo tinklo tvarkytojas per 4 mėnesius nuo 8 punkte nurodyto naudotojo pranešimo apie neatitiktį Tvarkos aprašo 5 punkte nurodytiems reikalavimams gavimo dienos negauna iš naudotojo 7 punkte nurodytos informacijos, apie tai informuoja naudotojo savininko teises ir pareigas įgyvendinančią instituciją ir Saugiojo tinklo valdytoją.

10. Saugiojo tinklo tvarkytojas ne vėliau kaip per 20 darbo dienų nuo Tvarkos aprašo 7 punkte nurodytos informacijos gavimo:

10.1. *Neteko galios nuo 2022-09-24*

Papunkčio naikinimas:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

10.2. vertina naudotojo pateiktą informaciją ir jei trūkumų nenustatyta – įtraukia naudotoją į prisijungimo prie Saugiojo tinklo planą, kuris tvirtinamas kiekvienų metų gruodžio mėnesį ateinantiems metams ir ne rečiau kaip kas ketvirtį peržiūrimas bei, esant poreikiui, atnaujinamas;

10.3. jei buvo nustatyta trūkumų, parengia šalintinų trūkumų sąrašą, nustato jų pašalinimo terminą, ne ilgesnį kaip 3 mėn., ir pateikia jį naudotojui.

11. Naudotojas apie pašalintus trūkumus informuoja Saugiojo tinklo tvarkytoją, ir jei trūkumų nenustatyta, yra įtraukiamas į prisijungimo prie Saugiojo tinklo planą.

12. Saugiojo tinklo tvarkytojas, pakartotinai nustatęs trūkumų, parengia trūkumų pašalinimo planą ir nustato ne ilgesnį kaip 10 darbo dienų terminą jiems pašalinti.

13. Naudotojui pakartotinai nepašalinus trūkumų per Saugiojo tinklo tvarkytojo nustatytą laiką, Saugiojo tinklo tvarkytojas ne vėliau kaip per 10 darbo dienų nuo termino pabaigos informuoja naudotojo savininko teises ir pareigas įgyvendinančią instituciją ir Saugiojo tinklo valdytoją apie naudotojo neatitiktį prijungimo prie Saugiojo tinklo reikalavimams ir negalėjimą prijungti tokio naudotojo prie Saugiojo tinklo.

14. Pagal prisijungimo prie Saugiojo tinklo planą, Saugiojo tinklo tvarkytojas vykdo Saugiojo tinklo paslaugoms pradėti teikti reikalingus darbus, kuriuos atlikus naudotojas ir Saugiojo tinklo tvarkytojas pasirašo prisijungimo prie Saugiojo tinklo aktą.

15. Prisijungimo prie Saugiojo tinklo akte, kurio formą tvirtina Saugiojo tinklo tvarkytojas, nurodoma:

15.1. Saugiojo tinklo tvarkytojas ir naudotojas;

15.2. naudotojo buveinės ir (ar) jo struktūrinių padalinių, esančių kitu nei buveinė adresu, jei juose bus prisijungiama prie Saugiojo tinklo, adresai;

15.3. naudotojo ir (ar) jo struktūrinių padalinių, esančių kitu nei buveinė adresu, patalpose įrengiama Saugiojo tinklo įranga;

15.4. Saugiojo tinklo įrangos įrengimo naudotojo patalpose vieta ar vietos;

15.5. naudotojo prisijungimo prie Saugiojo tinklo data, jei nesutampa su prisijungimo prie Saugiojo tinklo akto pasirašymo data;

15.6. naudotojui teikiamų paslaugų sąrašas bei jų kiekybiniai ir kokybiniai rodikliai;

15.7. Saugiojo tinklo tvarkytojo ir naudotojo įgalioti asmenys prisijungimo prie Saugiojo tinklo administravimo, saugos organizavimo ar įgyvendinimo klausimais.

16. Laikoma, kad naudotojas yra prisijungęs prie Saugiojo tinklo, kai Saugiojo tinklo tvarkytojas ir naudotojas pasirašo prisijungimo prie Saugiojo tinklo aktą.

17. Kai naudotojas turi struktūrinių padalinių kitose nei jo buveinė vietose, Tvarkos aprašo 5 punkto reikalavimai yra taikomi kiekvienam iš jų, jei juose bus įrengiama Saugiojo tinklo įranga, ir prisijungimo prie Saugiojo tinklo aktas su naudotoju pasirašomas tik nustačius visų nutolusių struktūrinių padalinių atitiktį Tvarkos aprašo 5 punkto reikalavimams.

18. Kai du ar daugiau naudotojų naudojasi tomis pačiomis patalpomis ir (ar) bendrais vietiniais tinklais (angl. *LAN*), esant techninei galimybei, įrengiamas vienas Saugiojo tinklo įvadas. Tokiu atveju Tvarkos aprašo 5 punkto reikalavimas taikomas tik naudotojui, kurio patalpose bus įrengta Saugiojo tinklo įranga.

19. Su naudotoju, kuris naudojasi kitų naudotojų patalpomis ir (ar) bendrais vietiniais tinklais, prisijungimo prie Saugiojo tinklo aktas pasirašomas tik tada, kai įvertinta naudotojo, kurio patalpose bus įrengiama Saugiojo tinklo įranga, atitiktis Tvarkos aprašo 5 punkte nustatytiems reikalavimams.

19^1. Kai naudotojo struktūrinis padalinys yra ne Lietuvos Respublikos teritorijoje, Tvarkos aprašo 5.1.2.1 ir 5.1.3 papunkčiuose nustatyti reikalavimai įgyvendinami pagal šalies, kurioje bus įrengta Saugiojo tinklo įranga, keliamus reikalavimus.

Papildyta punktu:
Nr. V-94, 2023-02-03, paskelbta TAR 2023-02-03, i. k. 2023-02047
Punkto pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

20. Naudotojas, kuris naudojasi kito naudotojo bendrais vietiniais tinklais, gali įgalioti šį naudotoją jo vardu pasirašyti prisijungimo prie Saugiojo tinklo aktą, taip pat jo vardu užsakyti paslaugų teikimą ar jas nutraukti.

21. Prieš pasikeičiant naudotojo prisijungimo prie Saugiojo tinklo vietos adresui ar prireikus prisijungti prie Saugiojo tinklo naujos vietos adresu, naudotojas ne vėliau kaip prieš 6 mėnesius turi pateikti Saugiojo tinklo tvarkytojui Tvarkos aprašo 7 punkte nurodytą informaciją, kiek ji yra susijusi su naujos prisijungimo prie Saugiojo tinklo vietos adresu nurodyta Saugiojo tinklo prieigos vieta.

22. Saugiojo tinklo tvarkytojas, gavęs 21 punkte nurodytą informaciją, naudotojui naują Saugiojo tinklo prieigos vietą suteikia *mutatis mutandis* taikydamas Tvarkos aprašo 10–16 punktus.

ANTRASIS SKIRSNIS
ATSIJUNGIMAS NUO SAUGIOJO TINKLO

23. Naudotojas, išbrauktas iš Saugiojo tinklo naudotojų sąrašo, netenka teisės naudotis Saugiuoju tinklu ir Saugiojo tinklo tvarkytojas per 10 darbo dienų kreipiasi į naudotoją dėl atjungimo nuo Saugiojo tinklo datos suderinimo, tada parengia atjungimo nuo Saugiojo tinklo planą.

24. Naudotojas privalo būti atjungtas ne vėliau kaip per 6 mėn. nuo išbraukimo iš Saugiojo tinklo naudotojų sąrašo dienos, o Saugiojo tinklo tvarkytojas ne vėliau kaip per 20 darbo dienų nuo naudotojo atjungimo nuo Saugiojo tinklo dienos privalo atsiimti iš naudotojo jo patalpose įrengtą Saugiojo tinklo įrangą.

25. Esant poreikiui nutraukti Saugiojo tinklo paslaugų teikimą naudotojo nurodytu adresu, naudotojas ne vėliau kaip prieš 2 mėnesius kreipiasi į Saugiojo tinklo tvarkytoją dėl paslaugų teikimo nutraukimo.

III SKYRIUS
PASLAUGŲ TEIKIMO SAUGIUOJU TINKLU SĄLYGOS

PIRMASIS SKIRSNIS
PASLAUGŲ UŽSAKYMAS

26. Saugiojo tinklo paslaugos naudotojams teikiamos tik prisijungus prie Saugiojo tinklo ir pasirašius prisijungimo prie Saugiojo tinklo aktą.

27. Standartinės paslaugos, nurodytos Tvarkos aprašo 1 priede, teikiamos naudotojui pagal prisijungimo prie Saugiojo tinklo akte nurodytus kiekybinius ir kokybinius rodiklius.

28. Naudotojas, siekiantis gauti standartinę paslaugą, užpildo Paslaugų užsakymo paraišką ir pateikia ją Saugiojo tinklo tvarkytojui.

29. Kalbinis ryšys teikiamas naudotojams pagal Tvarkos aprašo 3 priedo 1 punktą.

Punkto pakeitimai:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436
Nr. V-94, 2023-02-03, paskelbta TAR 2023-02-03, i. k. 2023-02047
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

29[1]. Valstybės mobilizacijos operacijų centro kalbiniu palydoviniu ryšiu bei Valstybės mobilizacijos operacijų centro prieiga prie viešųjų ryšių tinklų palydoviniu ryšiu turi teisę naudotis civilinės mobilizacijos institucijos, kurių vadovai ar jų įgalioti asmenys yra įtraukti į Valstybės mobilizacijos operacijų centro sudėtį, žvalgybos institucijos, taip pat Lietuvos Respublikos Prezidento kanceliarija, Lietuvos Respublikos Seimo kanceliarija. Naudotojui išduodamų SIM kortelių skaičius Valstybės mobilizacijos operacijų centro kalbiniam palydoviniam ryšiui užtikrinti bei Valstybės mobilizacijos operacijų centro prieigų prie viešųjų ryšių tinklų palydoviniu ryšiu suteikimo skaičius nurodyti Tvarkos aprašo 3 priedo 2 punkte.

Papildyta punktu:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

30. Standartinės paslaugos, nurodytos Tvarkos aprašo 1 priedo 4 ir 5 punktuose, užsakomos ir teikiamos naudotojui, jei šios paslaugos yra reikalingos naudotojo funkcijoms atlikti.

31. Naudotojas, siekiantis gauti Saugiuoju tinklu teikiamas papildomas paslaugas, užpildo Paslaugų užsakymo paraišką, nurodydamas pageidaujamus papildomų paslaugų kiekybinius rodiklius, ir ją pateikia Saugiojo tinklo tvarkytojui. Naudotojas taip pat turi teisę teikti Saugiojo tinklo tvarkytojui siūlymus dėl kitų papildomų paslaugų, nenurodytų Paslaugų užsakymo paraiškoje, teikimo.

32. Paslaugų teikimo pradžios terminai:

32.1. standartinės paslaugos, nurodytos Tvarkos aprašo 1 priedo 1–3 punktuose, pradedamos teikti ne vėliau kaip per 3 (tris) darbo dienas nuo prisijungimo prie Saugiojo tinklo akto arba jo pakeitimo pasirašymo;

32.2. standartinės paslaugos, nurodytos Tvarkos aprašo 1 priedo 4 ir 5 punktuose, pradedamos teikti ne vėliau kaip per 1 mėnesį nuo prisijungimo prie Saugiojo tinklo akto arba jo pakeitimo pasirašymo;

32.3. papildomos paslaugos pradedamos teikti per šalių susitartą terminą.

ANTRASIS SKIRSNIS
PASLAUGŲ KEITIMAS IR TEIKIMO NUTRAUKIMAS

33. Naudotojas turi teisę bet kada teikti naują Tvarkos aprašo 28 ar 31 punkte nurodytą paraišką arba jos dalį, kuri susijusi su keičiamos paslaugos kiekybiniais ir (ar) kokybiniais rodikliais.

34. Jeigu naudotojo funkcija, kuriai atlikti reikalinga standartinė paslauga, numatyta Tvarkos aprašo 1 priedo 4 ar 5 punkte, yra panaikinama, naudotojas ne vėliau kaip per 5 darbo dienas nuo šiame punkte nurodytos funkcijos panaikinimo dienos turi užpildyti Paslaugų užsakymo paraišką dėl turimos paslaugos teikimo nutraukimo ir pateikti ją Saugiojo tinklo tvarkytojui.

35. Saugiojo tinklo tvarkytojas, gavęs Tvarkos aprašo 34 punkte nurodytą informaciją, ne vėliau kaip per 10 darbo dienų ar per kitą šalių susitartą terminą nutraukia atitinkamos standartinės paslaugos, numatytos Tvarkos aprašo 1 priedo 4 ar 5 punkte, teikimą naudotojui, pasirašo su juo prisijungimo prie Saugiojo tinklo akto pakeitimą ir ne vėliau kaip per 20 darbo dienų atsiima iš naudotojo šiai paslaugai teikti įrengtą įrangą.

TREČIASIS SKIRSNIS
JUNGIMASIS PRIE VIEŠŲJŲ ELEKTRONINIŲ RYŠIŲ TINKLŲ NE PER SAUGŲJĮ TINKLĄ

35^1. Naudotojas gali jungtis prie viešųjų elektroninių ryšių tinklų ne per Saugųjį tinklą, kai yra bent viena iš šių sąlygų:

35^1.1. naudotojas, be gyvybiškai svarbios valstybės funkcijos užtikrinimo, kartu nuolat vykdo kitas visuomenės informavimo funkcijas ir jas vykdant dėl techninių priežasčių susidaro būtinybė prisijungti prie viešųjų elektroninių ryšių tinklų ne per Saugųjį tinklą;

35^1.2. naudotojas, be gyvybiškai svarbių valstybės funkcijų užtikrinimo ir mobilizacinių užduočių vykdymo, kartu organizuoja tarptautines pratybas ar kitus renginius ar juose dalyvauja ir

kai būtina užtikrinti Europos Sąjungos ar Šiaurės Atlanto sutarties organizacijos (NATO) šalims partnerėms prieigą prie viešųjų ryšių tinklų.

35^2. Naudotojas, norėdamas jungtis prie viešųjų elektroninių ryšių tinklų ne per Saugųjį tinklą, Saugiojo tinklo tvarkytojui raštu pateikia prašymą, kartu pateikdamas šią informaciją:

35^2.1. informaciją apie atitiktį bent vienai 35^1 punkto sąlygai;

35^2.2. naudojimosi viešųjų elektroninių ryšių tinklais trukmę, jei trukmė terminuota;

35^2.3. techninę prisijungimo prie viešųjų elektroninių ryšių tinklų dokumentaciją, pagrindžiančią atitiktį Tvarkos aprašo 38.13 papunkčiui.

35^3. Saugiojo tinklo tvarkytojas, gavęs Tvarkos aprašo 35^2 punkte nurodytą informaciją, ne vėliau kaip per 10 darbo dienų įvertina Saugiajam tinklui keliamas rizikas ir:

35^3.1. nenustatęs rizikų, raštu informuoja naudotoją apie suteiktą leidimą jungtis prie viešųjų elektroninių ryšių tinklų pagal kartu pridedamą ir su Saugiojo tinklo tvarkytoju suderintą techninį projektą;

35^3.2. nustatęs, kad jungtis prie viešųjų elektroninių ryšių tinklų kelia grėsmę Saugiojo tinklo saugumui ar gali kitaip trikdyti Saugiuoju tinklu teikiamas paslaugas, raštu informuoja apie tai naudotoją ir, kol bus suderinti techniniai sprendimai, nesuteikia leidimo jungtis prie viešųjų elektroninių ryšių tinklų.

Papildyta skirsniu:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

IV SKYRIUS
PASLAUGŲ TEIKIMO SAUGIUOJU TINKLU TAISYKLĖS

PIRMASIS SKIRSNIS
TEISĖS, PAREIGOS IR ATSAKOMYBĖ

36. Saugiojo tinklo tvarkytojo teisės:

36.1. be išankstinio perspėjimo, įvykus saugumo incidentui arba esant akivaizdžiai saugumo incidento grėsmei, sustabdyti paslaugos teikimą 48 val., apie paslaugos teikimo sustabdymą informuoti naudotoją per 1 darbo dieną;

36.2. pasitelkti trečiuosius asmenis įsipareigojimams vykdyti;

36.3. vertinti Tvarkos aprašo 5 punkto reikalavimų įgyvendinimą visą paslaugų teikimo laikotarpį.

37. Saugiojo tinklo tvarkytojo pareigos:

37.1. paskirti įgaliotą asmenį ar asmenis, kurie atstovaus Saugiojo tinklo tvarkytojui prisijungimo prie Saugiojo tinklo techninio administravimo klausimais, ir pateikti naudotojams šio asmens (asmenų) kontaktinius duomenis (vardą, pavardę, telefono numerį, elektroninio pašto adresą), o pasikeitus įgaliotiems asmenims ar kontaktinei informacijai atnaujintą informaciją ne vėliau kaip per 5 darbo dienas nuo įvykusių pasikeitimų dienos pateikti naudotojams;

37.2. įrengti, prižiūrėti, keisti bei išmontuoti Saugiojo tinklo įrangą ir šalinti jos sutrikimus;

37.3. ne mažiau kaip prieš 3 darbo dienas įspėti naudotoją apie planinius Saugiojo tinklo įrangos remonto ar priežiūros darbus, planuojamų darbų datą, laiką ir trukmę;

37.4. imtis priemonių, kurios užtikrintų Saugiojo tinklo ir paslaugų saugumą, vientisumą, prieinamumą, paslaugų suderinamumą;

37.5. nustačius arba gavus informacijos, kad naudotojas nesilaiko Visuomenės informavimo, Autorių teisių ir gretutinių teisių įstatymuose ir kitų teisės aktuose įtvirtintų reikalavimų arba sudaro sąlygas juos pažeisti tretiesiems asmenims, informuoti apie tai naudotoją ir imtis visų reikalingų priemonių, siekiant apriboti tokių pažeidimų pasireiškimo galimybes Saugiajame tinkle;

37.6. šalinti paslaugų teikimo sutrikimus, jeigu paslaugos teikimo kiekybiniai ir kokybiniai rodikliai neatitinka nurodytų prisijungimo prie Saugiojo tinklo akte.

38. Naudotojo pareigos:

38.1. užtikrinti Tvarkos aprašo 5 punkto reikalavimų įgyvendinimą visą paslaugų teikimo laikotarpį;

38.2. pranešti raštu Saugiojo tinklo tvarkytojui apie bet kokius pasikeitimus, susijusius su naudotojo teisinio statuso, pavadinimo, adreso ar kitų rekvizitų pasikeitimais ar patikslinimais, per 5 darbo dienas nuo pakeitimų atsiradimo dienos;

38.3. užtikrinti, kad naudotojo patalpose esančios Saugiojo tinklo tvarkytojo elektroninių ryšių linijos, Saugiojo tinklo įranga nebūtų sugadintos, pažeistos, sunaikintos dėl naudotojo ar trečiųjų asmenų kaltės, ne vėliau kaip per 1 darbo dieną pranešti Saugiojo tinklo tvarkytojui apie bet kokius veiksmus, lėmusius įrangos praradimą, sugadinimą ir kt. Naudotojui draudžiama savavališkai taisyti Saugiojo tinklo įrangą ir (ar) ją modifikuoti, išmontuoti, perkelti ar atlikti kitus veiksmus;

38.4. užtikrinti galimybę Saugiojo tinklo tvarkytojo atstovams, atliekantiems Saugiojo tinklo įrangos įrengimo, priežiūros, remonto ar gedimų šalinimo darbus, patekti į patalpas, kuriose yra Saugiojo tinklo įranga, ir įsinešti / išsinešti įrankius, medžiagas, Saugiojo tinklo įrangą ir jos dalis, matavimo įrangą, reikalingus minėtiems darbams atlikti;

38.5. vykdyti Saugiojo tinklo tvarkytojo nurodymus, būtinus Saugiojo tinklo ir paslaugų teikimo teisėtumui ir saugumui užtikrinti;

38.6. ne vėliau kaip per 1 darbo dieną informuoti Saugiojo tinklo tvarkytoją apie paslaugos teikimo sutrikimus;

38.7. informuoti Saugiojo tinklo tvarkytoją apie planinius naudotojo tinklo techninės priežiūros darbus ir (ar) žinomus galimus elektros energijos tiekimo sutrikimus prieš 3 darbo dienas, jei šie darbai ar sutrikimai gali turėti įtakos paslaugų teikimui;

38.8. atsiskaityti su Saugiojo tinklo tvarkytoju už papildomas paslaugas pagal pateiktas sąskaitas;

38.9. užtikrinti, kad prie Saugiojo tinklo būtų jungiama techniškai su Saugiuoju tinklu suderinama naudotojo elektroninių ryšių įranga;

38.10. užtikrinti, kad naudotojo informacinių išteklių tarnybinės stotys, vartotojų darbo vietų kompiuteriai ir kita įranga, kuri siųs ir gaus duomenis per Saugųjį tinklą, turėtų vidinius IP adresus naudotojo tinkle. Vidiniai naudotojo kompiuterių tinklo adresai negali būti iš IP adresų srities 10.200.X.X–10.255.X.X, išskyrus atskirus atvejus, prieš tai suderinus su Saugiojo tinklo tvarkytoju;

38.11. naudoti tik Saugiojo tinklo domenų vardų sistemos (angl. DNS) IP adresus;

Papildyta papunkčiu:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

38.12. dalyvauti Saugiojo tinklo valdytojo ir (ar) tvarkytojo organizuojamuose Saugiojo tinklo veiklos tęstinumo išbandymuose.

Papildyta papunkčiu:

Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

38.13. prie viešųjų elektroninių ryšių tinklų jungiantis ne per Saugųjį tinklą:

38.13.1. fiziškai atskirti Saugųjį tinklą nuo jungčių su kitais elektroninių ryšių tinklais;

38.13.2. Saugiojo tinklo naudotojų įrangos (tinklo įrenginiai, kompiuteriai ir kt.) nejungti tuo pačiu metu ir prie Saugiojo tinklo, ir prie kito tuo metu naudojamo viešųjų elektroninių ryšių tinklo.

Papildyta papunkčiu:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

ANTRASIS SKIRSNIS
PASLAUGŲ TEIKIMO SUSTABDYMO SĄLYGOS

39. Paslaugų teikimas naudotojui ribojamas arba, esant grėsmei pažeisti Saugųjį tinklą ar padaryti žalos Saugiajam tinklui arba kitiems naudotojams, stabdomas, jei:

39.1. naudotojas nesiima veiksmų grėsmėms ir saugos incidentų pasekmėms pašalinti savo valdomame tinkle ir tai kelia grėsmę Saugiajam tinklui ir kitų Saugiojo tinklo naudotojų tinklų saugai;

39.2 paslaugų teikimo laikotarpiu nustatoma neatitiktis Tvarkos aprašo 5 punkto reikalavimams;

39.3. naudotojas atliko veiksmus, kurie galėjo pažeisti Saugųjį tinklą arba sukelti grėsmę, kad Saugusis tinklas gali būti pažeistas, ar padaryti žalos Saugiajam tinklui arba kitiems naudotojams. Vertinant grėsmes stebimas su Saugiuoju tinklu susijusių sistemų arba prisijungusių naudotojų sistemų informacijos, duomenų perdavimo paslaugų ar infrastruktūros konfidencialumo, prieinamumo ar vientisumo pažeidžiamumo pokytis.

40. Naudotojui laiku neatsiskaičius su Saugiojo tinklo tvarkytoju už suteiktas papildomas paslaugas, stabdomas šių papildomų paslaugų teikimas.

41. Sprendimą dėl paslaugų teikimo sustabdymo ar ribojimo priima Saugiojo tinklo tvarkytojas ir raštu įspėja naudotoją 39.1–39.3 papunkčiuose nurodytais atvejais ne vėliau kaip prieš 3 darbo dienas, o 40 punkte nurodytu atveju – ne vėliau kaip prieš 20 darbo dienų iki paslaugų teikimo sustabdymo dienos.

42. Saugiojo tinklo tvarkytojui sustabdžius ar apribojus paslaugų teikimą naudotojui, paslaugų teikimas neatnaujinamas tol, kol nepanaikinamos sustabdymą sukėlusios priežastys. Saugiojo tinklo tvarkytojas paslaugų teikimą atnaujina ne vėliau kaip kitą dieną, kai naudotojas pašalina paslaugų teikimo sustabdymą ar ribojimą sukėlusias priežastis ir apie tai informuoja Saugiojo tinklo tvarkytoją. Tvarkos aprašo 39.1, 39.3 papunkčiuose nurodytais atvejais paslaugų teikimas turi būti atnaujintas gavus informaciją iš NKSC apie grėsmių Saugiajam tinklui sukelto incidento išsprendimą.

43. Saugiojo tinklo tvarkytojas, nepagrįstai sustabdęs papildomų paslaugų teikimą, neskaičiuoja mokesčių už papildomas paslaugas per paslaugų teikimo sustabdymo laikotarpį.

44. Dėl naudotojo kaltės sustabdžius paslaugų teikimą, naudotojas neatleidžiamas nuo mokesčių už papildomų paslaugų teikimą mokėjimo.

TREČIASIS SKIRSNIS
MOKĖJIMAS UŽ PAPILDOMŲ PASLAUGŲ TEIKIMĄ

45. Atlyginimo už papildomas paslaugas dydžiai nurodyti Tvarkos aprašo 4 priede.

46. Naudotojas atsiskaito su Saugiojo tinklo tvarkytoju už papildomą paslaugą kas mėnesį, ne vėliau kaip per 30 kalendorinių dienų nuo sąskaitos pateikimo naudotojui dienos.

47. Naudotojas, užsisakęs papildomas kalbinio ryšio paslaugas (skambučius į miesto, mobiliojo ryšio telefonų numerius, peradresavimą į mobiliojo ryšio numerius), taip pat viršijęs Valstybės mobilizacijos operacijų centro kalbinio palydovinio ryšio standartinio paslaugų plano limitą (50 Eur) arba užsakęs skubų pristatymą, atsiskaito pagal faktines tokių paslaugų gavimo išlaidas.

Punkto pakeitimai:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436
Nr. V-94, 2023-02-03, paskelbta TAR 2023-02-03, i. k. 2023-02047
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

PATVIRTINTA
Lietuvos Respublikos
krašto apsaugos ministro
2019 m. liepos 2 d.
įsakymu Nr. V-583

SPECIALIŲJŲ ORGANIZACINIŲ IR TECHNINIŲ REIKALAVIMŲ, TAIKOMŲ SAUGIAJAM VALSTYBINIAM DUOMENŲ PERDAVIMO TINKLUI, JUO TEIKIAMOMS PASLAUGOMS BEI PREKIŲ IR PASLAUGŲ SAUGIAJAM VALSTYBINIAM DUOMENŲ PERDAVIMO TINKLUI TEIKĖJAMS, APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Specialiųjų organizacinių ir techninių reikalavimų, taikomų Saugiajam valstybiniam duomenų perdavimo tinklui, juo teikiamoms paslaugoms bei prekių ir paslaugų Saugiajam valstybiniam duomenų perdavimo tinklui teikėjams, aprašas (toliau – Aprašas) nustato specialiuosius organizacinius ir techninius reikalavimus Saugiajam valstybiniam duomenų perdavimo tinklui (toliau – Saugusis tinklas), Saugiuoju tinklu teikiamoms paslaugoms bei prekių ir paslaugų Saugiajam tinklui teikėjams.

2. Saugiojo tinklo tvarkytojas, pirkdamas paslaugas, darbus ar įrangą, susijusius su Saugiuoju tinklu, jo projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, pirkimo dokumentuose turi nustatyti, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas turi atitikti Apraše ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. nutarimu Nr. 1209 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, nustatytus reikalavimus.

3. Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos kibernetinio saugumo, Lietuvos Respublikos viešųjų pirkimų įstatymuose, šių įstatymų įgyvendinamuosiuose teisės aktuose, taip pat Informacinių technologijų paslaugų valdymo metodikoje, patvirtintoje Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2013 m. birželio 19 d. įsakymu Nr. T-83 „Dėl Informacinių technologijų paslaugų valdymo metodikos patvirtinimo“.

II SKYRIUS
ORGANIZACINIAI REIKALAVIMAI

4. Saugiojo tinklo tvarkytojas turi paskirti:

4.1. Saugiojo tinko administratorių (administratorius), prižiūrintį Saugųjį tinklą ir jo

infrastruktūrą, užtikrinantį jo veikimą ir elektroninės informacijos saugą;

4.2. Saugiojo tinko saugos įgaliotinį, koordinuojantį ir prižiūrintį saugos politikos įgyvendinimą.

5. Saugiojo tinklo tvarkytojas turi parengti ir pateikti tvirtinti Saugiojo tinklo valdytojui:

5.1. Saugiojo tinklo nuostatus, kuriuos sudaro šie skyriai:

5.1.1. „I skyrius. Bendrosios nuostatos“, kuriame nurodomas steigimo teisinis pagrindas, tikslas, uždaviniai, funkcijos, teisės aktai, kuriais vadovaujantis kuriamas ir tvarkomas Saugusis tinklas;

5.1.2. „II skyrius. Organizacinė struktūra“, kuriame nustatoma organizacinė struktūra: valdytojas, tvarkytojai, duomenų subjektai, jų funkcijos, teisės ir pareigos;

Papunkčio pakeitimai:
Nr. V-94, 2023-02-03, paskelbta TAR 2023-02-03, i. k. 2023-02047

5.1.3. „III skyrius. Informacinė struktūra“, kuriame nustatoma informacinė struktūra: gaunami, kaupiami, tvarkomi ir teikiami duomenys, duomenų grupės ir (arba) informacija;

5.1.4. „IV skyrius. Funkcinė struktūra“, kuriame nustatoma funkcinė struktūra: sudedamosios dalys ir jų atliekamos funkcijos, nurodomos Saugiojo tinklo teikiamos paslaugos;

5.1.5. „V skyrius. Duomenų sauga ir jų teikimas“, kuriame reglamentuojama duomenų sauga ir duomenų teikimas: nurodomas duomenų saugojimo duomenų bazėje terminas, nustatoma, kada ir kaip šie duomenys perkeliami į duomenų bazės archyvą, kiek laiko saugomi šiame archyve, taip pat nurodomi veiksmai, atliekami pasibaigus nustatytam terminui, duomenų teikimo sąlygos;

Papunkčio pakeitimai:
Nr. V-94, 2023-02-03, paskelbta TAR 2023-02-03, i. k. 2023-02047

5.1.6. „VI skyrius. Modernizavimas ir likvidavimas“, kuriame nustatoma modernizavimo ir likvidavimo tvarka;

5.2. Saugiojo tinklo specifikaciją, kurią sudaro šie skyriai:

5.2.1. „I skyrius. Bendrosios nuostatos“, kuriame nustatoma: steigimo pagrindą nurodantys teisės aktai, numatytą kompiuterizuoti veiklos sritį reglamentuojantys teisės aktai, duomenų saugą reglamentuojantys teisės aktai;

5.2.2. „II skyrius. Veiklos reikalavimai“, kuriame grafiškai atvaizduojama Saugiojo tinklo funkcinė schema, aprašomi išoriniai ir vidiniai duomenų srautai, nurodant šaltinį, duomenų srauto identifikatorių, aprašoma duomenų bazių struktūra, atitikties tarptautiniams ir geros praktikos standartams reikalavimai, reikalavimai techninėms priemonėms, veikimo charakteristikoms, programinei įrangai, realizavimo technologijoms;

5.2.3. „III skyrius. Techninė ir programinė įranga“, kuriame nurodytas leistinos programinės įrangos sąrašas, techninės įrangos sąrašas, techninės ir programinės įrangos parametrai ir už šios

įrangos priežiūrą atsakingas asmuo (asmenys), minimalaus funkcionalumo įrangos, tinkamos veiklai užtikrinti įvykus saugos incidentui, specifikacija;

5.2.4. „IV skyrius. Patalpos“, kuriame nurodyti kiekvieno pastato, kuriame yra įranga, aukšto patalpų brėžiniai ir juose pažymėtos tarnybinės stotys; kompiuterių tinklo ir telefonų tinklo mazgai; kompiuterių tinklo ir telefonų tinklo laidų vedimo tarp pastato aukštų vietos; elektros įvedimo pastate vietos; Saugiojo tinklo fizinio ir loginio sujungimo schemos; programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos; už šiame papunktyje nurodytų dokumentų parengimą atsakingo asmens pareigos;

5.2.5. „V skyrius. Priemonės“, kuriame aprašomos Saugiojo tinklo paslaugų teikimo priemonės; eksploatavimo ir priežiūros priemonės; naudotojų identifikavimo ir autentifikavimo priemonės; fizinės apsaugos priemonės; priemonės, susijusios su Saugiojo tinklo personalu; priemonės, susijusios su Saugiojo tinklo programine įranga; programinės ir techninės įrangos saugaus konfigūravimo taisyklės ir pagrindinės naudojimo nuostatos; nuotolinio prisijungimo būdai ir protokolai, keitimosi elektronine informacija formatai, šifravimo metodai; prieigos teisių valdymo ir kontrolės priemonės; Saugiojo tinklo tvarkytojo veiksmų ir Saugiojo tinklo įvykių registravimo priemonės; incidentų, pokyčių ir problemų valdymo priemonės; įsibrovimų aptikimo ir prevencijos priemonės bei už šių priemonių naudojimą ir kontrolę atsakingi asmenys, jų funkcijos;

5.2.6. „VI skyrius. Sutartys“, kuriame nurodytos elektroninės informacijos teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutartys, atsakingų už šių sutarčių įgyvendinimo priežiūrą asmenų pareigos; jei Saugiojo tinklo tvarkytojas naudoja (pagal nuomos, panaudos ar kitas sutartis) techninę įrangą ar jos dalį, priklausančias ir esančias trečiosios šalies patalpose, – sutarties su trečiąja šalimi data ir numeris; už šių sutarčių saugojimą atsakingų asmenų pareigos;

5.2.7. „VII skyrius. Sąnaudos ir nauda“, kuriame aprašomos planuojamos naudojimo ir priežiūros sąnaudos, prognozuojama finansinė, ekonominė ir socialinė nauda;

5.3. Saugiojo tinklo naudotojų administravimo taisykles, kurias sudaro šie skyriai:

5.3.1. „I skyrius. Bendrosios nuostatos“, kuriame nustatomi subjektai, kuriems bus taikomos šios taisyklės, prieigos prie elektroninės informacijos principai;

5.3.2. „II skyrius. Naudotojų ir administratorių įgaliojimai, teisės ir pareigos“, kuriame nustatomi naudotojų ir administratorių įgaliojimai, teisės ir pareigos; administratoriaus (administratorių) prieigos lygiai ir juose taikomi saugos reikalavimai;

5.3.3. „III skyrius. Saugaus elektroninės informacijos teikimo naudotojams kontrolės tvarka“, kuriame nustatoma tvarka, kuria bus registruojami ir išregistruojami naudotojai, ir už šių veiksmų atlikimą atsakingas asmuo; priemonės naudotojų tapatybei nustatyti; naudotojų

slaptažodžių sudarymo, galiojimo trukmės ir keitimo reikalavimai; sąlygos ir atvejai, kai panaikinamos naudotojų teisės; leistini nuotolinio naudotojų prisijungimo būdai;

5.4. Saugiojo tinklo veiklos tęstinumo planą, kurį sudaro šie skyriai:

5.4.1. „I skyrius. Bendrosios nuostatos“, kuriame nustatoma, kad planas įsigalioja įvykus saugos incidentui; naudotojų ir kitų asmenų įgaliojimai ir veiksmai pagal planą; finansinių ir kitokių išteklių, numatomų veiklai atkurti įvykus saugos incidentui, šaltiniai; veiklos kriterijai, pagal kuriuos galima nustatyti, ar veikla atkurta;

5.4.2. „II skyrius. Organizacinės nuostatos“, kuriame nustatoma veiklos tęstinumo valdymo grupės sudėtis (vadovas, pavaduotojas ir kiti nariai); veiklos atkūrimo grupės sudėtis (vadovas, pavaduotojas ir kiti nariai); veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės narių sąrašas su kontaktiniais duomenimis, leidžiančiais pasiekti šiuos asmenis bet kuriuo metu; veiklos atkūrimo detalusis planas, kuriame nurodytas veiksmų vykdymo eiliškumas, terminai, atsakingi vykdytojai; numatant atskirus plano scenarijus veiklai atkurti po skirtingo pobūdžio ir masto saugos incidentų; reikalavimai, keliami atsarginėms patalpoms, naudojamoms veiklai atkurti po saugos incidentų, atsarginių patalpų adresas ir būdai, kaip iki jų nuvykti; veiklos tęstinumo valdymo grupės ir veiklos atkūrimo valdymo grupės komunikavimo reikalavimai (dažnumas, formos ir kita); veiklos tęstinumo valdymo ir veiklos atkūrimo grupės funkcijos:

5.4.2.1. situacijos analizė ir sprendimų veiklos tęstinumo valdymo klausimais priėmimas;

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

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

5.4.2.4. bendravimas su teisėsaugos ir kitomis institucijomis, Saugiojo tinklo valdytojo ir tvarkytojo valstybės tarnautojais, darbuotojais, dirbančiais pagal darbo sutartis, bei profesinės karo tarnybos kariais (toliau – darbuotojai) ir kitomis interesų grupėmis;

5.4.2.5. finansinių ir kitų išteklių, reikalingų veiklai atkurti, įvykus saugos incidentui, naudojimo kontrolė;

5.4.2.6. elektroninės informacijos fizinė sauga įvykus saugos incidentui;

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

5.4.2.8. veiklos atkūrimo priežiūra ir koordinavimas;

5.4.2.9. tarnybinių stočių veikimo atkūrimo organizavimas;

5.4.2.10. tinklo veikimo atkūrimo organizavimas;

5.4.2.11. elektroninės informacijos atkūrimo organizavimas;

5.4.2.12. taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

5.4.2.13. darbo kompiuterių veikimo atkūrimo ir prijungimo tinklo organizavimas;

5.4.3. „III skyrius. Plano veiksmingumo išbandymo nuostatos“, kuriame nustatomas plano

veiksmingumo paskutinio ir kito planuojamo išbandymo būdas ir periodiškumas; asmuo, atsakingas už išbandant plano veiksmingumą pastebėtų trūkumų ataskaitos parengimą ir pateikimą Saugiojo tinklo valdytojui; išbandant plano veiksmingumą pastebėtų trūkumų šalinimo principai.

5.5. Saugiojo tinklo incidentų, pokyčių ir problemų valdymo tvarkos aprašą, kurį sudaro šie skyriai (reikalavimai incidentų valdymo tvarkos turiniui taikomi ir pokyčių valdymo tvarkos turiniui):

5.5.1. „I skyrius. Incidentų valdymo proceso ryšys su kitais paslaugų valdymo procesais“, kuriame nurodoma, kokia informacija, sukaupta incidentų valdymo proceso metu, turi būti pateikta problemų, keitimų, sąrankos valdymo procesų dalyviams;

5.5.2. „II skyrius. Incidentų valdymo proceso dalyviai“, kuriame nurodomi incidentų valdymo proceso dalyviai, jiems paskirtos funkcijos ir pareigybės arba struktūriniai vienetai, galintys atlikti tam tikras funkcijas;

5.5.3. „III skyrius. Incidentų būsenos“, kuriame išskiriamos ir aprašomos būsenos, kurios žymi esminių incidento valdymo etapų atlikimą;

5.5.4. „IV skyrius. Incidentų valdymo proceso schema ir proceso įgyvendinimo metu atliekami veiksmai“, kuriame incidentų valdymo procesas pavaizduojamas grafine schema, pateikiami atliekamų veiksmų aprašymai bei nurodomi vykdytojai;

5.5.5. „V skyrius. Incidentų kategorijų sąrašas“, kuriame aprašomos galimos sutrikimų kategorijos ir jų aprašymai. Incidentų kategorijos gali atspindėti teikiamas paslaugas arba infrastruktūros sritis;

5.5.6. „VI skyrius. Incidentų prioritetai“, kuriame nurodomos galimos incidentų šalinimo prioriteto reikšmės. Incidento prioritetas nustatomas vadovaujantis incidento įtakos mastu, kuris nurodo, kaip plačiai atitinkamas incidentas paveikia teikiamas paslaugas, bei incidento skubumu, kuris nurodo, kaip skubiai atitinkamas incidentas turi būti pašalintas;

5.5.7. „VII skyrius. Incidentų šalinimo požymių sąrašas“, kuriame nurodomi sutrikimų šalinimo požymiai bei jų aprašymai;

5.5.8. „VIII skyrius. Incidentų valdymo proceso matavimo rodikliai“, kuriame nurodomi valdymo proceso efektyvumui matuoti naudojami rodikliai; vykdytojai, atsakingi už matavimo rodiklių kaupimą ir teikimą; incidentų valdymo proceso matavimo rodiklių teikimo periodiškumas; vykdytojai, atsakingi už incidentų valdymo proceso matavimo rodiklių analizę bei reagavimo veiksmų vykdymą.

5.6. Saugiojo tinklo kibernetinio saugumo politiką, kurią sudaro šie skyriai:

5.6.1. „I skyrius. Bendrosios nuostatos“, kuriame nurodomas politikos tikslas ir taikymo apimtis, kibernetinio saugumo valdymo kryptys, atsakomybių pasiskirstymas;

5.6.2. „II skyrius. Audito žurnalų duomenų administravimas ir saugojimas“, kuriame aprašoma audito žurnalų duomenų administravimo ir saugojimo tvarka;

5.6.3. „III skyrius. Įsibrovimų aptikimas ir prevencija“, kuriame aprašoma Saugiojo tinklo įsibrovimų aptikimo, vertinimo tvarka;
5.6.4. „IV skyrius. Mobiliųjų įrenginių naudojimas ir kontrolė“, kuriame nustatomi Saugiojo tinklo veiklai ir paslaugoms teikti naudojamų mobiliųjų įrenginių saugos reikalavimai, jų laikymosi kontrolė;
5.6.5. „V skyrius. Grėsmių ir pažeidžiamumų valdymas“, kuriame nustatoma Saugiojo tinklo grėsmių ir pažeidžiamumų skenavimo, rezultatų vertinimo ir klasifikavimo tvarka, pažeidžiamumų nustatymo plano rengimo, pažeidžiamumų nustatymo programinės įrangos naudojimo bei nustatytų trūkumų šalinimo nuostatos;
5.6.6. „VI skyrius. Kibernetinių incidentų valdymas“, kuriame aprašomas kibernetinio incidento valdymo organizavimas: nustatymas, vertinimas, stabdymas ir šalinimas;
5.6.7. „VII skyrius. Kibernetinio saugumo priemonės“, kuriame nurodomos kibernetiniam saugumui Saugiajame tinkle užtikrinti naudojamos techninės ir programinės priemonės, šių priemonių diegimas ir parametrų keitimas;
5.6.8. „VIII skyrius. Mokymai“, kuriame nustatoma Saugiojo tinklo tvarkytojo darbuotojų švietimo informacijos saugos klausimais organizavimo tvarka, Saugiojo tinklo naudotojų informavimas saugos klausimais.
Papildyta papunkčiu:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

6. Saugiojo tinklo tvarkytojo darbuotojų pareiginėse instrukcijose ir pareigybių aprašymuose turi būti numatytos jų funkcijos, susijusios su Saugiojo tinklo sauga, priežiūra, administravimu, prieigos prie Saugiojo tinklo suteikimu bei Saugiuoju tinklu teikiamų paslaugų teikimu.

7. Saugiojo tinklo tvarkytojo darbuotojai, prekių ir paslaugų Saugiajam tinklui teikėjai su Saugiojo tinklo tvarkytoju turi pasirašyti konfidencialumo sutartis, užtikrinančias, kad jokia informacija, gauta iš Saugiojo tinklo tvarkytojo, nebus atskleista trečiosioms šalims.

8. Saugiojo tinklo tvarkytojo darbuotojai, prieš pradėdami darbą su Saugiuoju tinklu, turi būti supažindinti su Saugiojo tinklo saugą reglamentuojančiais teisės aktais.

III SKYRIUS
TECHNINIAI REIKALAVIMAI

9. Techniniai reikalavimai Saugiuoju tinklu teikiamoms paslaugoms:

9.1. Turi būti paskirti asmenys, atsakingi už paslaugų, nurodytų krašto apsaugos ministro patvirtintame Prisijungimo prie Saugiojo valstybinio duomenų perdavimo tinklo, atsijungimo nuo jo ir elektroninių ryšių paslaugų teikimo šiuo tinklu tvarkos apraše (toliau – paslaugos), valdymo procesą, paslaugų kokybę.

9.2. Turi būti stebimi paslaugų teikimo kiekybiniai ir kokybiniai rodikliai (toliau – paslaugų teikimo rodikliai), pasikeitus patvirtintoms reikšmėms, informuojamas asmuo, atsakingas už paslaugų kokybę.

9.3. Paslaugų teikimo rodiklių stebėjimas ir atsakingų asmenų informavimas turi būti automatizuotas.

9.4. Saugiojo tinklo tvarkytojas teikia informaciją Saugiojo tinklo valdytojui apie paslaugų teikimo rodiklių pasikeitimus per metus.

10. Techniniai reikalavimai identifikavimo ir autentifikavimo priemonėms:

10.1. Turi būti užtikrintas prie Saugiojo tinklo prijungtos techninės įrangos atpažinimas.

10.2. Naudotojo prieiga prie Saugiojo tinklo turi būti galima tik iš Saugiojo tinklo prisijungimo ir paslaugų teikimo aktuose nurodytos techninės įrangos.

10.3. Techninei įrangai atpažinti turi būti naudojamos įrangos atpažinimo žymos, viešųjų raktų infrastruktūra.

10.4. Prieigos prie Saugiojo tinklo teisių ir priemonių suteikimas, pakeitimas ar panaikinimas Saugiojo tinklo tvarkytojo darbuotojams turi būti registruojamas Saugiojo tinklo valdytojo tvirtinamų Saugiojo tinklo naudotojų administravimo taisyklių nustatyta tvarka.

11. Techniniai reikalavimai fizinei apsaugai ir įsibrovimų prevencijai:

11.1. Patekimas į patalpas, kuriose sumontuota Saugiojo tinklo įranga (toliau – patalpos), ir teritorijas, kuriose yra patalpos (toliau – teritorijos), turi būti kontroliuojamas fizinėmis ir techninėmis prieigos kontrolės priemonėmis.

11.2. Asmenys, patenkantys į patalpas ir teritorijas, turi būti identifikuojami.

11.3. Asmenys, esantys patalpose ir teritorijose, visą laiką turi segėti tapatybę patvirtinančias korteles arba svečių leidimus.

11.4. Turi būti kaupiama informacija apie asmenų patekimo į patalpas ir teritorijas datą ir laiką.

11.5. Saugiojo tinklo tvarkytojo darbuotojų įeigos kontrolės sistema turi užtikrinti, kad darbuotojai į patalpas ir teritorijas pateks vienu iš būdų:

11.5.1. savarankiškai atrakinę durų mechaninį užraktą raktu;

11.5.2. perėję turniketus ar vartelius, stebimus už patalpų ir teritorijų apsaugą atsakingo asmens tiesiogiai arba per vaizdo stebėjimo sistemą.

11.6. Asmenys, esantys patalpose ar teritorijose, kurie nėra Saugiojo tinklo tvarkytojo darbuotojai, turi būti lydimi darbuotojų visą jų buvimo patalpose ir teritorijose laiką.

11.7. Kompiuterinė ir ryšio įranga turi būti įnešama arba išnešama iš patalpų ir teritorijų tik Saugiojo tinklo tvarkytojo įgaliotų asmenų.

11.8. Turi būti vykdoma patalpų durų, patalpose esančių seifų, metalinių spintų raktų bei užraktų, elektroninių apsaugos sistemų kodų išdavimo ir jų keitimo kontrolė, apsauga.

11.9. Techniniai reikalavimai įsibrovimų aptikimui ir prevencijai:

11.9.1. turi būti vykdoma apsauga nuo įsibrovimo, naudojamos vaizdo stebėjimo sistemos neteisėtam patekimui į patalpas ir (arba) teritorijas aptikti;

11.9.2. patalpose ir (arba) teritorijose turi būti įrengta nuolat veikianti apsaugos nuo įsibrovimo sistema;

11.9.3. už priskirtų patalpų ir teritorijų apsaugą atsakingas asmuo turi reaguoti į apsaugos nuo įsibrovimo sistemos pranešimą ir į įsibrovimo vietą atvykti ne vėliau kaip per 15 min.

11.10. Fizinei apsaugai užtikrinti naudojamos apsaugos priemonės turi atitikti reikalavimus, nurodytus Saugiojo valstybinio duomenų perdavimo tinklo fizinės ir veiklos apsaugos reikalavimų apraše, patvirtintame Lietuvos Respublikos krašto apsaugos ministro 2019 m. balandžio 1 d. įsakymu Nr. V-328 „Dėl Asmenų, kuriems dėl jiems priskirtų funkcijų ar pavesto darbo suteikiama teisė be palydos patekti prie Kertinio valstybės telekomunikacijų centro tvarkomos Saugiojo valstybinio duomenų perdavimo tinklo infrastruktūros arba priimti sprendimus dėl šios infrastruktūros funkcionavimo, pareigų sąrašo ir Saugiojo valstybinio duomenų perdavimo tinklo fizinės ir veiklos apsaugos reikalavimų aprašo patvirtinimo“.

Papunkčio pakeitimai:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

11.11. *Neteko galios nuo 2022-09-24*
Papunkčio naikinimas:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

11.12. *Neteko galios nuo 2022-09-24*
Papunkčio naikinimas:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

12. Techniniai reikalavimai programinės įrangos priemonėms:

12.1. Programinė įranga gali būti diegiama tik gavus patvirtinimą Saugiojo tinklo tvarkytojo nustatyta Saugiojo tinklo pokyčių valdymo tvarka.

12.2. Turi būti įdiegtos elektroninės informacijos šifravimo, apsaugos nuo kenksmingojo programinio kodo priemonės.

12.3. Turi būti įdiegtos ir nuolatos atnaujinamos apsaugos priemonės nuo kenkimo programinės įrangos.

12.4. Turi būti įdiegtos priemonės, užtikrinančios, kad elektroninė informacija perdavimo metu nebūtų pakeista, būtų patvirtinta elektroninės informacijos siuntėjo ir gavėjo tapatybė, elektroninė informacija perdavimo metu nebūtų perimta.

12.5. Turi būti naudojamos užkardos, atitinkančios EAL4 lygį pagal standartą ISO/IEC 15408 ir laikantis šio standarto reikalavimų. Periodiškai turi būti peržiūrimi užkardų įrašai, siekiant įvertinti bandymus sutrikdyti Saugiojo tinklo veiklą.

12.6. Privaloma laikytis programinės įrangos licencijose nustatytų nurodymų.

12.7. Draudžiama naudoti nelicencijuotą programinę įrangą.

12.8. Nelegali programinė įranga turi būti šalinama, nustatant jos atsiradimo šaltinį.

12.9. Ilgiau kaip metus nenaudojama Saugiojo tinklo programinė įranga turi būti šalinama.

12.10. Elektroninės informacijos laikmenos prieš jas naudojant turi būti patikrintos, ar jose

nėra kenkimo programinės įrangos.

12.11. Saugiojo tinklo prijungimai prie viešųjų ryšių tinklų turi būti atliekami per vieną pagrindinį įrenginį ir apsaugoti užkarda.

12.12. Ne rečiau kaip kartą per mėnesį turi būti įvertinami kibernetiniam saugumui užtikrinti naudojamų priemonių programiniai atnaujinimai, klaidų taisymai ir šie atnaujinimai diegiami.

13. Techniniai reikalavimai Saugiojo tinklo tvarkytojo darbuotojų veiksmų ir Saugiojo tinklo įvykių registravimui:

13.1. Turi būti registruojami Saugiojo tinklo techninės ir programinės įrangos nustatymų pakeitimai, jie turi būti tvirtinami Saugiojo tinklo tvarkytojo nustatyta Saugiojo tinklo pokyčių valdymo tvarka.

13.2. Turi būti registruojami saugos incidentai, Saugiojo tinklo valdymo sistemos ar kitų Saugiojo tinklo saugą užtikrinančių sistemų pavojaus signalai.

13.3. Turi būti atliekamas Saugiojo tinklo tvarkytojo darbuotojo veiksmų registravimas.

14. Reikalavimai Saugiojo tinklo pokyčių valdymui:

14.1. Saugiojo tinklo pokyčiai turi būti valdomi Saugiojo tinklo tvarkytojo patvirtinta tvarka.

14.2. Visa informacija apie pokyčius turi būti saugoma ir valdoma vienoje informacinėje sistemoje. Detali informacija apie pokytį ir jo būseną turi būti įrašoma ir atnaujinama laiku.

14.3. Turi būti paskirtas asmuo, atsakingas už pokyčių valdymo procesą, bei asmenys, atsakingi už Saugiojo tinklo kiekvienos paslaugos pokyčių valdymą, analizę ir sprendimą.

14.4. Turi būti paskirti asmenys arba sudaryti komitetai, atsakingi už pokyčių tvirtinimą bei skubių pokyčių tvirtinimą.

14.5. Nepatvirtinti pokyčiai negali būti vykdomi, neįgalioti asmenys negali atlikti pokyčio.

14.6. Vienas kitam prieštaraujantys pakeitimai ar pakeitimai, dėl kurių gali sutrikti Saugiojo tinklo veikla, negali būti vykdomi.

14.7. Pakeitimai turi būti išbandomi testavimo aplinkoje.

14.8. Saugiojo tinklo tvarkytojas sudaro ir patvirtina standartinių ir tipinių pokyčių sąrašus, nustato jų vykdymo procedūras.

14.9. Saugiojo tinklo techninės, programinės ir komunikacinės įrangos nustatymai, parametrai ir konfigūracija turi atitikti nustatytus Saugiojo tinklo specifikacijoje.

14.10. Nepavykus įgyvendinti Saugiojo tinklo pakeitimo, turi būti imtasi atkūrimo veiksmų.

15. Reikalavimai incidentų (įskaitant ir saugos incidentus) valdymui:

15.1. Saugiojo tinklo incidentai turi būti valdomi pagal Saugiojo tinklo tvarkytojo nustatytą tvarką.

15.2. Incidentų valdymas turi būti automatizuotas.

15.3. Visa informacija apie incidentus turi būti saugoma ir valdoma vienoje informacinėje sistemoje. Detali informacija apie incidentą ir jo būseną turi būti įrašoma ir atnaujinama laiku.

15.4. Visiems incidentams turi būti taikoma standartinė klasifikacijos sistema Saugiojo tinklo valdytojo nustatyta Saugiojo tinklo incidentų valdymo tvarka.

15.5. Turi būti nustatytas reakcijos į incidentus laikas bei incidentų išsprendimo laikas.

15.6. Visi incidentų įrašai turi turėti vienodus informacijos laukus ir formatą.

15.7. Turi būti paskirtas asmuo, atsakingas už incidentų valdymo procesą, bei asmenys, atsakingi už Saugiojo tinklo kiekvienos paslaugos incidentų valdymą, analizę ir sprendimą.

15.8. Turi būti kaupiama žinių bazė, kurioje saugoma aktuali informacija apie problemas ir incidentus, susijusius su Saugiuoju tinklu, ir jų sprendimo būdus.

15.9. Informacija apie incidentus ir jų būseną turi būti perduodama ir paslaugų gavėjams, kurių veikla sutrinka dėl incidento, ir sprendžiantiems incidentus. Informacija turi būti pateikiama suprantamais terminais.

15.10. Turi būti prieiga prie incidentų, žinių bazės, konfigūracijos informacijos, padedančių efektyviai įrašyti, suskirstyti incidentus ir atlikti jų analizę.

15.11. Įrašai apie incidentus turi būti peržiūrimi kas savaitę, kontroliuojant, ar jiems teisingai suteiktos kategorijos ir užpildyta visa reikalinga informacija.

16. Reikalavimai problemų valdymui:

16.1. Problemų ir incidentų valdymas turi būti atskirtas.

16.2. Saugiojo tinklo problemos turi būti valdomos Saugiojo tinklo tvarkytojo nustatyta tvarka.

16.3. Visa informacija apie problemas turi būti saugoma ir valdoma vienoje informacinėje sistemoje. Detali informacija apie problemą ir jo būseną turi būti įrašoma ir atnaujinama laiku.

16.4. Visoms problemoms turi būti taikoma standartinė klasifikacijos sistema Saugiojo tinklo valdytojo nustatyta Saugiojo tinklo problemų valdymo tvarka.

16.5. Visi problemų įrašai turi turėti vienodus informacijos laukus ir formatą.

16.6. Turi būti paskirtas asmuo, atsakingas už problemų valdymo procesą, ir asmenys, atsakingi už Saugiojo tinklo kiekvienos paslaugos problemų valdymą, analizę ir sprendimą.

17. Reikalavimai atitikties kibernetinio saugumo reikalavimų ir rizikos vertinimui, Saugiojo tinklo techninės ir programinės įrangos inventorizavimui:

17.1. Saugiojo tinklo tvarkytojas kasmet atlieka Saugiojo tinklo rizikos vertinimą Krašto apsaugos sistemos ryšių ir informacinių sistemų rizikos vertinimo ir valdymo tvarkos aprašo, patvirtinto Lietuvos Respublikos krašto apsaugos ministro 2008 m. liepos 18 d. įsakymu Nr. V-685 „Dėl Krašto apsaugos sistemos informacinių sistemų rizikos vertinimo ir valdymo tvarkos aprašo

patvirtinimo“, nustatyta tvarka, parengia ir pateikia Saugiojo tinklo valdytojui tvirtinti Saugiojo tinklo rizikos įvertinimo ataskaitą, rizikos įvertinimo ir rizikos valdymo priemonių planą.

17.2. Saugiojo tinklo tvarkytojas kasmet atlieka Saugiojo tinklo atitikties kibernetinio saugumo reikalavimams ir šiame Apraše nustatytiems reikalavimams patikrą, parengia ir pateikia Saugiojo tinklo valdytojui tvirtinti patikros ataskaitą ir trūkumų šalinimo planą.

17.3. *Neteko galios nuo 2023-06-01*
Papunkčio naikinimas:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

17.4. Saugiojo tinklo tvarkytojas kasmet atlieka Saugiojo tinklo veiklos tęstinumo valdymo plano veiksmingumo patikrinimą, parengia ir patvirtina ataskaitą apie pastebėtus plano veiksmingumo trūkumus, pasiūlo šių trūkumų šalinimo priemones.

17.5. Saugiojo tinklo tvarkytojas kasmet atlieka Saugiojo tinklo techninės ir programinės įrangos inventorizavimą ir teikia informaciją Saugiojo tinklo valdytojui apie atliktus veiksmus ir nustatytus trūkumus. Inventorizavimo metu:

17.5.1. nustatomas techninės įrangos išdėstymas;

17.5.2. fiksuojamos techninės įrangos charakteristikos;

17.5.3. sudaromas ar atnaujinamas techninės įrangos inventorizacijos aprašas;

17.5.4. peržiūrimas leistinos programinės įrangos sąrašas;

17.5.5. patikrinama, ar sisteminė ir taikomoji programinė įranga legali ir saugi;

17.5.6. patikrinama, ar įdiegti operacinių sistemų ir naudojamos taikomosios programinės įrangos gamintojų rekomenduojami atnaujinimai.

PATVIRTINTA
Lietuvos Respublikos
krašto apsaugos ministro
2021 m. kovo 25 d.
įsakymu Nr. V-207

SAUGIOJO TINKLO NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Saugiojo tinklo naudotojų administravimo taisyklės (toliau – Administravimo taisyklės) nustato prieigos prie Saugiojo valstybinio duomenų perdavimo tinklo (toliau – Saugusis tinklas) elektroninės informacijos principus, Saugiojo tinklo naudotojų (toliau – Naudotojai), Saugiojo tinklo administratorių (toliau – Administratoriai) įgaliojimus, teises, pareigas, saugaus elektroninės informacijos teikimo Naudotojams kontrolės tvarką.

2. Administravimo taisyklėse vartojamos sąvokos:

2.1. Paslaugų valdymo priemonių naudotojas – Naudotojo įgaliotas asmuo prisijungimo prie Saugiojo tinklo administravimo, saugos organizavimo ar įgyvendinimo klausimams spręsti, turintis prieigos teisę prie Saugiojo tinklo valdymo priemonių;

2.2. Administravimo taisyklėse vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo 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“, ir kituose duomenų saugų tvarkymą reglamentuojančiuose teisės aktuose.

3. Prieigos prie Saugiojo tinklo elektroninės informacijos principai:

3.1. būtinumo principas – suteikiama tik tiek prieigos prie Saugiojo tinklo, kiek tai būtina funkcijoms atlikti;

3.2. leistinumo principas – galimi tik tie veiksmai, kuriuos atlikti yra suteikta teisė Saugiojo tinklo saugą reglamentuojančiuose dokumentuose;

3.3. prieinamumo ribojimo principas – susipažinti su Saugiojo tinklo saugoma elektronine informacija ir ją tvarkyti gali tik tie Administratoriai, kuriems tokia teisė buvo suteikta;

3.4. apskaitos principas – Saugiajame tinkle atliekami Naudotojų darbuotojų ir Administratorių veiksmai turi būti registruojami, užtikrinant veiksmus atlikusių asmenų tapatybės nustatymą.

II SKYRIUS
NAUDOTOJŲ IR ADMINISTRATORIŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

4. Naudotojų įgaliojimus, teises ir pareigas nustato Prisijungimo prie Saugiojo valstybinio duomenų perdavimo tinklo, atsijungimo nuo jo ir elektroninių ryšių paslaugų teikimo šiuo tinklu tvarkos aprašas, patvirtintas Lietuvos Respublikos krašto apsaugos ministro 2019 m.

liepos 2 d. įsakymu Nr. V-583 „Dėl Saugiojo valstybinio duomenų perdavimo tinklo veiklą užtikrinančių dokumentų patvirtinimo“, ir šios Administravimo taisyklės.

5. Naudotojai turi užtikrinti, kad jų darbuotojai nedelsdami praneštų asmeniui, įgaliotam atstovauti Naudotojui prisijungimo prie Saugiojo tinklo administravimo, saugos organizavimo ir įgyvendinimo klausimais, arba Saugiojo tinklo tvarkytojui apie:

5.1. Saugiojo tinklo sutrikimus;

5.2. saugos politikos pažeidimus;

5.3. nusikalstamos veiklos Saugiajame tinkle požymius;

5.4. neveikiančias ar netinkamai veikiančias kibernetinio saugumo ir elektroninės informacijos saugos užtikrinimo priemones;

5.5. neįprastą Saugiojo tinklo veikimą;

5.6. esamus arba galimus informacijos saugumo reikalavimų pažeidimus bei kitų Naudotojų darbuotojų veiksmus, atliekamus nesilaikant Administravimo taisyklių ar kitų teisės aktų.

6. Naudotojo darbuotojams draudžiama savavališkai rinkti, tvarkyti, perduoti, saugoti, naikinti ar kitaip naudoti elektroninę informaciją apie Saugųjį tinklą.

7. Paslaugų valdymo priemonių naudotojas turi teisę:

7.1. pranešti apie gaunamų Saugiojo tinklo paslaugų sutrikimus;

7.2. užsakyti naujas paslaugas;

7.3. užsakyti gaunamų paslaugų keitimus.

8. Administratoriai pagal savo atsakomybę Saugiajame tinkle skirstomi į:

8.1. tinklo komponentų administratorius;

8.2. tarnybinių stočių administratorius;

8.3. kibernetinio saugumo administratorius;

8.4. paslaugų valdymo priemonių administratorius.

9. Tinklo komponentų administratorius turi šias teises ir pareigas:

9.1. administruoti kolektyvinės apsaugos kibernetinio saugumo priemones ir vykdyti jų priežiūrą;

9.2. administruoti tinklo įrangą;

9.3. administruoti sujungimus su viešaisiais ryšių tinklais ir vykdyti jų priežiūrą;

9.4. administruoti valstybės valdomų elektroninių ryšių tinklų, kurie naudojami vykdant valstybines mobilizacines užduotis, dalių sujungimus;

9.5. administruoti sąveiką su Europos Sąjungos ir jos valstybių narių institucijų valdomais informaciniais ištekliais ir vykdyti priežiūrą;

9.6. administruoti elektroninių ryšių infrastruktūrą.

10. Tarnybinių stočių administratorius turi šias teises ir pareigas:

10.1. administruoti tarnybines stotis ir duomenų bazes;

10.2. administruoti srities vardų struktūrą (angl. *Domain Name System* (DNS);

10.3. vykdyti virtualizacijos platformos priežiūrą;

10.4. valdyti tarnybinių stočių rezervines kopijas;

10.5. atnaujinti ir prižiūrėti programinę įrangą;

10.6. administruoti kibernetinio saugumo priemones ir vykdyti jų priežiūrą.

11. Kibernetinio saugumo administratorius turi šias teises ir pareigas:

11.1. stebėti Saugiojo tinklo saugą kibernetinės saugos priemonėmis;

11.2. tirti ir analizuoti kibernetinius incidentus;

11.3. vertinti Saugiojo tinklo pažeidžiamumą;

11.4. administruoti kibernetinio saugumo priemones administravimą ir vykdyti jų priežiūrą.

12. Paslaugų valdymo priemonių administratorius turi šias teises ir pareigas:

12.1. administruoti naudotojų ir jų įgaliotų darbuotojų duomenis;

12.2. vykdyti Saugiuoju tinklu teikiamų paslaugų apskaitą;

12.3. valdyti Saugiajame tinkle vykstančius incidentus, problemas ir pokyčius.

13. Naudotojų darbuotojai ir Administratoriai privalo laikytis saugos dokumentuose ir kituose teisės aktuose nustatytų reikalavimų.

III SKYRIUS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO NAUDOTOJAMS KONTROLĖS TVARKA

14. Administratoriai yra skiriami Saugiojo tinklo tvarkytojo įsakymu Saugiojo tinklo saugos įgaliotinio teikimu.

15. Prieigą prie paslaugų valdymo priemonių Paslaugų valdymo priemonių naudotojui suteikia paslaugų valdymo priemonių administratorius.

16. Kiti Naudotojų darbuotojai Saugiojo tinklo tvarkytojo nėra registruojami.

17. Paslaugų valdymo priemonių naudotojų registravimo tvarka:

17.1. Naudotojo darbuotojas Saugiojo tinklo tvarkytojui teikia su Naudotojo vadovu suderintą prašymą suteikti prieigą prie paslaugų valdymo priemonių;

17.2. Paslaugų valdymo priemonių administratorius ne vėliau kaip per 10 darbo dienų nuo prašymo gavimo dienos suteikia Paslaugų valdymo priemonių naudotojui atskirą ir nesikartojantį prisijungimo vardą ir laikiną slaptažodį;

17.3. Paslaugų valdymo priemonių naudotojo prieigos teisės nedelsiant, bet ne vėliau kaip per 1 darbo dieną sustabdomos, kai paslaugų valdymo priemonių administratorius gauna informaciją apie:

17.3.1. Paslaugų valdymo priemonių naudotojo funkcijų, kurioms vykdyti buvo suteikta prieiga, pasikeitimą;

17.3.2. nutrūkus Paslaugų valdymo priemonių naudotojo, kuriam buvo suteikta prieiga prie paslaugų valdymo priemonės, darbo santykiams;

17.3.3. Naudotojo statuso netekimą.

18. Paslaugų valdymo priemonių naudotojų slaptažodžių saugos reikalavimai:

18.1. laikinas slaptažodis turi būti perduodamas atskirai nuo prisijungimo vardo;

18.2. pirmojo prisijungimo metu Paslaugų valdymo priemonių naudotojui privaloma pasikeisti laikinąjį slaptažodį;

18.3. kilus įtarimui, kad slaptažodis galėjo būti atskleistas, Paslaugų valdymo priemonių naudotojo slaptažodis nedelsiant turi būti pakeistas;

18.4. slaptažodį Paslaugų valdymo priemonių naudotojui privaloma įsiminti, draudžiama slaptažodį užsirašyti ar atskleisti kitam asmeniui;

18.5. slaptažodis turi būti ne trumpesnis nei 10 simbolių bei sudarytas iš raidžių, skaičių ir specialiųjų simbolių;

Papunkčio pakeitimai:
Nr. V-94, 2023-02-03, paskelbta TAR 2023-02-03, i. k. 2023-02047

18.6. slaptažodžiams sudaryti neturi būti naudojama asmeninė informacija (vardas, pavardė, gimimo data, šeimos narių vardai ir pan.);

18.7. slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius.

19. Paslaugų valdymo priemonių naudotojui tris kartus iš eilės neteisingai įvedus slaptažodį, prisijungimas turi būti automatiškai blokuojamas.

20. Paslaugų valdymo priemonių naudotojas, pamiršęs slaptažodį, privalo kreiptis į paslaugų valdymo priemonių administratorių, kuris suteikė prisijungimo vardą ir pirminį slaptažodį.

21. Kiekvienas Paslaugų valdymo priemonių naudotojas privalo naudoti tik jam suteiktą prisijungimo vardą. Naudoti svetimą prisijungimo vardą draudžiama.

21.[1] Paslaugų valdymo priemonių naudotojui 15 minučių neatliekant jokių veiksmų Paslaugų valdymo priemonėje, naudotojas automatiškai atjungiamas ir vėl jungtis prie Paslaugų valdymo priemonės gali tik pakartotinai patvirtinęs savo tapatybę.

Papildyta punktu:
Nr. V-94, 2023-02-03, paskelbta TAR 2023-02-03, i. k. 2023-02047

22. Saugiojo tinklo administratorių skyrimo ir prieigos prie Saugiojo tinklo suteikimo tvarka:

22.1. Saugiojo tinklo saugos įgaliotinis arba kitas Saugiojo tinklo tvarkytojo vadovo įgaliotas asmuo parengia įsakymo dėl Administratoriaus paskyrimo projektą ir teikia jį Saugiojo tinklo tvarkytojui pasirašyti;

Papunkčio pakeitimai:
Nr. V-94, 2023-02-03, paskelbta TAR 2023-02-03, i. k. 2023-02047

22.2. Administratoriui prieigos prie Saugiojo tinklo teisės suteikiamos arba pakeičiamos nuo įsakymo įsigaliojimo dienos;

22.3. Administratoriaus prieigos prie Saugiojo tinklo teisės sustabdomos nedelsiant, bet ne vėliau kaip per 1 darbo dieną, kai Saugiojo tinklo saugos įgaliotinis gauna informaciją apie:

22.3.1. Administratoriaus nušalinimą nuo darbo (pareigų) teisės aktų nustatytais atvejais;

22.3.2. Administratoriaus neatitiktį pareigybės aprašyme nustatytiems kvalifikaciniams reikalavimams;

22.3.3. nesinaudojimą prieigos prie Saugiojo tinklo teise ilgiau nei 2 mėnesius;

22.3.4. nustatytą faktą, kad prieigos prie Saugiojo tinklo teisės naudojamos pažeidžiant Saugiojo tinklo elektroninės informacijos saugą ir kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytus reikalavimus.

22.[1] Saugiojo tinklo saugos įgaliotinis arba kitas Saugiojo tinklo tvarkytojo vadovo įgaliotas asmuo ne rečiau kaip kartą per metus atlieka prieigos teisių peržiūrą.

Papildyta punktu:
Nr. V-94, 2023-02-03, paskelbta TAR 2023-02-03, i. k. 2023-02047

23. Nutrūkus darbo santykiams, Administratoriaus prieigos teisės turi būti panaikinamos paskutinę Administratoriaus darbo dieną, tačiau ne vėliau kaip iki darbo dienos pabaigos.

24. Administratoriaus prieigos teisės panaikinamos Saugiojo tinklo tvarkytojo įsakymu.

25. Administratoriai savo funkcijas privalo vykdyti naudodami tam skirtą atskirą paskyrą.

26. Administratoriui darbo stotyje, iš kurios administruojamas Saugusis tinklas, neatliekant jokių veiksmų, darbo stotis turi užsirakinti, kad toliau administruoti Saugųjį tinklą būtų galima tik pakartotinai patvirtinus savo tapatybę. Laikas, per kurį Administratoriui neatliekant jokių veiksmų darbo stotis užsirakina, negali būti ilgesnis kaip penkiolika minučių.

27. Administratorių slaptažodžių reikalavimai:

27.1. slaptažodį turi sudaryti ne mažiau kaip 12 simbolių;

27.2. slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių;

27.3. slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (vardas, pavardė, mergautinė pavardė, gimimo data, šeimos narių vardai ir pan.);

27.4. slaptažodžių savininkai turi užtikrinti slaptažodžių konfidencialumą (jų saugojimą paslaptyje ir neatskleidimą kitiems darbuotojams ar tretiesiems asmenims).

28. Saugiojo tinklo dalys, atliekančios nutolusio prisijungimo autentifikavimą ar patvirtinančios Administratoriaus tapatumą, turi drausti automatiškai išsaugoti slaptažodžius.

29. *Neteko galios nuo 2023-02-04*

Punkto naikinimas:
Nr. V-94, 2023-02-03, paskelbta TAR 2023-02-03, i. k. 2023-02047

30. Administratorius, pamiršęs slaptažodį, privalo kreiptis į saugos įgaliotinį arba į jo įgaliotą asmenį, kuris suteikė prisijungimo vardą ir pirminį slaptažodį.

31. Kilus įtarimui, kad slaptažodis galėjo būti atskleistas, slaptažodžio savininkas turi nedelsdamas pakeisti slaptažodį ir apie tai informuoti Saugiojo tinklo saugos įgaliotinį.

32. Saugos įgaliotinis arba jo įgaliotas asmuo turi užtikrinti, kad:

32.1. slaptažodis būtų keičiamas ne rečiau kaip kas 2 mėnesius;

32.2. slaptažodžio savininkas pirminį slaptažodį privalomai pasikeistų pirmojo prisijungimo metu;

32.3. slaptažodžio savininkas iš anksto (prieš 10 dienų) būtų perspėjamas apie jo slaptažodžio galiojimo pabaigą;

32.4. renkantis ar keičiant slaptažodį būtų reikalavimas bent kartą jį pakartoti;

32.5. būtų įsimenami paskutiniai 6 naudoti slaptažodžiai ir neleidžiama rinktis iš šio sąrašo;

32.6. jungiantis prie Saugiojo tinklo administravimo darbo stoties ir tris kartus iš eilės neteisingai įvedus slaptažodį, prisijungimas turi būti automatiškai blokuojamas.

33. Slaptažodžiai privalo būti saugomi, jų šifravimui taikant saugius šifravimo algoritmus.

33.[1] Prisijungimo vardai ir slaptažodžiai negali būti perduodami jų gavėjams tame pačiame elektroniniame laiške.

Papildyta punktu:
Nr. V-94, 2023-02-03, paskelbta TAR 2023-02-03, i. k. 2023-02047

34. Draudžiama Saugiojo tinklo techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti pakeisti ir atitikti 27 punkte nurodytus reikalavimus.

35. Nuotolinis prisijungimas prie Saugiojo tinklo turi būti atliekamas pagal protokolą, skirtą duomenims šifruoti.

36. Administratoriai administruoti Saugųjį tinklą gali tik jungdamiesi iš Saugiajam tinklui administruoti skirtos darbo stoties.

Papildyta priedu:
Nr. V-207, 2021-03-25, paskelbta TAR 2022-12-05, i. k. 2022-24736

PATVIRTINTA
Lietuvos Respublikos
krašto apsaugos ministro
2021 m. balandžio 22 d.
įsakymu Nr. V-286

SAUGIOJO TINKLO VEIKLOS TĘSTINUMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Saugiojo tinklo veiklos tęstinumo planas (toliau − Planas) reglamentuoja Saugiojo valstybinio duomenų perdavimo tinklo (toliau – Saugusis tinklas) veiklos ir juo teikiamų paslaugų tęstinumo valdymą, Saugiojo tinklo veiklos atkūrimą.

Punkto pakeitimai:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

2. Plane vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo, Lietuvos Respublikos kibernetinio saugumo, Lietuvos Respublikos elektroninių ryšių įstatymuose, šių įstatymų įgyvendinamuosiuose teisės aktuose.

3. Planas aktyvuojamas įvykus elektroninės informacijos saugos incidentui arba bet kokiam kitam įvykiui ar veiksmui, numatytam Plano 1 priede (toliau – Saugos inicidentas).

4. Saugiojo tinklo saugos įgaliotinis atsakingas už Plano ir su juo susijusių dokumentų parengimą.

5. Saugiojo tinklo veikla ir paslaugos laikomos atkurtos, jei tenkina Prisijungimo prie Saugiojo valstybinio duomenų perdavimo tinklo, atsijungimo nuo jo ir elektroninių ryšių paslaugų teikimo šiuo tinklu tvarkos aprašo, patvirtinto Lietuvos Respublikos krašto apsaugos ministro 2019 m. liepos 2 d. įsakymu Nr. V-583 „Dėl Saugiojo valstybinio duomenų perdavimo tinklo veiklą užtikrinančių dokumentų patvirtinimo“, 1 priede nurodytus kiekybinius ar kokybinius rodiklius.

Punkto pakeitimai:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

6. Saugiojo tinklo veiklos atkūrimas finansuojamas iš Lietuvos valstybės biudžeto ir kitų teisės aktuose numatytų finansavimo šaltinių.

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

7. Saugiojo tinklo veiklos ir juo teikiamų paslaugų tęstinumui valdyti ir atkūrimui organizuoti sudaromos dvi grupės:

Punkto pakeitimai:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

7.1. Veiklos tęstinumo valdymo grupė (toliau – Valdymo grupė);

7.2. Veiklos atkūrimo grupė (toliau – Atkūrimo grupė).

8. Valdymo grupę sudaro:

8.1. vadovas – Kertinio valstybės telekomunikacijų centro direktorius;

8.2. vadovo pavaduotojas – Saugumo skyriaus vedėjas;

8.3. nariai:

8.3.1. Veiklos valdymo departamento (toliau – VVD) direktorius;

8.3.2. VVD Valdymo organizavimo skyriaus vedėjas;

8.3.3. VVD Aptarnavimo ir paslaugų valdymo skyriaus vedėjas;

8.3.4. Saugiojo tinklo saugos įgaliotinis;

8.3.5. Tinklo technologijų departamento (toliau – TTD) direktorius;

8.3.6. TTD Tinklo valdymo skyriaus vedėjas;

8.3.7. TTD Tinklo paslaugų teikimo skyriaus vedėjas;

8.3.8. Informacinių technologijų skyriaus vedėjas.

Punkto pakeitimai:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

9. Atkūrimo grupę sudaro:

9.1. vadovas – TTD direktorius;

9.2. pavaduotojas – TTD Tinklo valdymo skyriaus vedėjas;

9.3. nariai:

9.3.1. visi TTD darbuotojai;

9.3.2. visi Informacinių technologijų skyriaus informacinių technologijų sistemų administratoriai;

Papunkčio pakeitimai:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

9.3.3. visi Saugumo skyriaus informacinių technologijų ir ryšių saugumo specialistai.

Papunkčio pakeitimai:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

10. Valdymo grupė:

10.1. atlieka saugos incidento sukeltos situacijos analizę;

10.2. priima sprendimus dėl konkrečių priemonių incidento poveikiui sustabdyti taikymo, siekiant sumažinti jo daromą žalą;

10.3. bendrauja su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;

10.4. bendrauja su susijusių informacinių sistemų veiklos tęstinumo valdymo grupėmis;

10.5. bendrauja su teisėsaugos ir kitomis institucijomis, Saugiojo tinklo valdytojo ir tvarkytojo valstybės tarnautojais, darbuotojais, dirbančiais pagal darbo sutartis, bei profesinės karo tarnybos kariais (toliau – darbuotojai) ir kitomis interesų grupėmis;

10.6. vykdo finansinių ir kitų išteklių, reikalingų veiklai atkurti įvykus saugos incidentui, naudojimo kontrolę;

10.7. užtikrina elektroninės informacijos fizinę saugą įvykus saugos incidentui;

10.8. esant būtinumui, organizuoja logistiką (žmonių, daiktų, įrangos gabenimą);

10.9. prižiūri ir koordinuoja veiklos atkūrimą.

11. Akūrimo grupė:

11.1. organizuoja Saugiojo tinklo tarnybinių stočių veikimo atkūrimą;

11.2. organizuoja Saugiojo tinklo veikimo ir juo teikiamų paslaugų atkūrimą;

Papunkčio pakeitimai:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

11.3. organizuoja elektroninės informacijos atkūrimą;

11.4. organizuoja taikomųjų programų atkūrimą;

11.5. organizuoja darbo kompiuterių veikimo atkūrimą ir jų prijungimą prie tinklo.

12. Valdymo grupės ir Atkūrimo grupės vadovų ir narių kontaktiniai duomenys, leidžiantys pasiekti šiuos asmenis bet kuriuo metu, tvirtinami Kertinio valstybės telekomunikacijų centro direktoriaus įsakymu.

Punkto pakeitimai:
Nr. V-94, 2023-02-03, paskelbta TAR 2023-02-03, i. k. 2023-02047

13. Įvykus Saugos incidentui Valdymo grupės vadovas nedelsdamas, bet ne vėliau kaip per 24 valandas nuo informacijos apie saugos incidentą gavimo, organizuoja Valdymo grupės susirinkimą.

14. Valdymo grupė, atlikusi situacijos analizę, nedelsdama, bet ne vėliau kaip per 2 valandas, susisiekia su Atkūrimo grupės vadovu ir informuoja jį apie esamą padėtį bei priimtus sprendimus dėl veiklos atkūrimo.

15. Tarpusavyje Valdymo grupės ir Atkūrimo grupės nariai bendrauja asmeniškai, elektroniniu paštu, mobiliaisiais telefonais arba kitomis priemonėmis ne rečiau kaip kas valandą.

16. Apie įvykdytus veiklos atkūrimo etapus Atkūrimo grupės nariai nedelsdami informuoja Atkūrimo grupės vadovą.

17. Atkūrimo grupės vadovas nuolat informuoja Valdymo grupės vadovą apie veiklos atkūrimo eigą.

18. Reaguojant į Saugos incidentus ir juos valdant, turi būti vadovaujamasi Plano 1 priede pateiktu Saugiojo tinklo veiklos atkūrimo detaliuoju planu veiklai ir paslaugoms atkurti po skirtingo pobūdžio ir masto saugos incidentų.

Punkto pakeitimai:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

19. Atsarginėms patalpoms, naudojamoms Saugiojo tinklo veiklai ir paslaugoms atkurti po Saugos incidentų, taikomi šie reikalavimai:“

Punkto pakeitimai:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

19.1. patalpos turi būti tokio dydžio, kad tilptų Saugiojo tinklo veiklai atkurti būtina įranga;

19.2. turi būti įrengti elektros srovės, kompiuterių tinklo ir telekomunikacijos prievadai;

19.3. turi būti įrengta patalpų kondicionavimo sistema;

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

19.5. patalpose turi būti užtikrintas patikimas elektros energijos tiekimas per nenutrūkstamo maitinimo šaltinius.

20. Atsarginių patalpų adresas ir būdai, kaip iki jų nuvykti, nustatomi Saugiojo tinklo tvarkytojo.

Punkto pakeitimai:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

III SKYRIUS
PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

21. Planas turi būti išbandomas ne rečiau kaip kartą per metus.

22. Plano veiksmingumas išbandomas stalo ar kitokių simuliacinių pratybų būdu.

Punkto pakeitimai:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

23. Plano veiksmingumo išbandymo būdas ir data nustatomi metiniame Kertinio valstybės telekomunikacijų centro veiklos plane.

24. Plano išbandymą organizuoja Valdymo grupės vadovas.

25. Po Plano veiksmingumo išbandymo Saugiojo tinklo saugos įgaliotinis ne vėliau kaip per 30 dienų parengia Saugiojo tinklo veiklos tęstinumo plano veiksmingumo išbandymo metu pastebėtų trūkumų ataskaitą (Plano 2 priedas), kurioje būtų numatytos priemonės trūkumams pašalinti, ir pateikia ją pasirašyti Valdymo grupės vadovui.

26. Plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami vadovaujantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

27. Valdymo grupės vadovas Saugiojo tinklo veiklos tęstinumo plano veiksmingumo išbandymo metu pastebėtų trūkumų ataskaitą ne vėliau kaip per 5 darbo dienas po šio dokumento priėmimo dienos pateikia Saugiojo tinklo valdytojui, kopiją – Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos.

Punkto pakeitimai:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

Papildyta priedu:
Nr. V-286, 2021-04-22, paskelbta TAR 2021-04-22, i. k. 2021-08376

Saugiojo tinklo veiklos
tęstinumo plano
1 priedas

SAUGIOJO TINKLO VEIKLOS ATKŪRIMO DETALUSIS PLANAS VEIKLAI IR PASLAUGOMS ATKURTI PO SKIRTINGO POBŪDŽIO IR MASTO SAUGOS INCIDENTŲ“

Eil. Nr.	Saugos incidentas	Veiksmai eilės tvarka		Terminas	Atsakingi vykdytojai
1.	Telekomunikacijų ryšio paslaugų teikimo sutrikimai	1.1.	Telekomunikacijų ryšio paslaugų teikėjų informavimas apie ryšio paslaugų sutrikimus, sutrikimo pašalinimo prognozės ir rekomendacijų gavimas	Nedelsiant, bet ne vėliau kaip per 15 min.	Valdymo grupės vadovas
		1.2.	Klientų informavimas apie paslaugų teikimo sutrikimus ir numatomą sutrikimų pašalinimo terminą	Nedelsiant, bet ne vėliau kaip per 15 min.	Valdymo grupė
		1.3.	Ryšio sutrikimo sukeltų pasekmių likvidavimo priemonių plano sudarymas, jei yra būtinybė	Ne vėliau kaip per 1,5 val.	Valdymo grupė Atkūrimo grupė
		1.4.	Sukeltų pasekmių likvidavimas	Priklausomai nuo atkūrimo darbų apimties – nuo 3 kalendorių dienų iki 2 mėnesių	Atkūrimo grupė
2.	Patalpų užgrobimas	2.1.	Teisėsaugos tarnybų informavimas, jei nebuvo informuota	Nedelsiant	Valdymo grupės vadovas
		2.2	Klientų informavimas (jei yra galimybė) apie galimus paslaugų teikimo sutrikimus ir numatomą sutrikimų pašalinimo terminą	Nedelsiant, bet ne vėliau kaip 15 min.	Valdymo grupė

		2.3.	Darbuotojų evakavimo galimybių nagrinėjimas ir sprendimo priėmimas, jei yra teisėsaugos tarnybų rekomendacijos	Ne vėliau kaip per 1 val.	Valdymo grupė
		2.4.	Darbuotojų informavimas apie evakavimą, jei priimtas toks sprendimas	Ne vėliau kaip per 1,5 val.	Valdymo grupė
		2.5	Padarytos žalos įvertinimas ir priemonių plano sudarymas	Atgavus patalpas ne vėliau kaip per 2 d. d.	Valdymo grupė Atkūrimo grupė
		2.6.	Padarytos žalos likvidavimas	Atgavus patalpas, priklausomai nuo atkūrimo darbų apimties – nuo 3 d. d. iki 2 mėn.	Atkūrimo grupė
3.	Elektros energijos tiekimo sutrikimas	3.1.	Elektros energijos tiekimo tarnybos informavimas	Nedelsiant, bet ne vėliau kaip per 15 min.	Valdymo grupės vadovas
		3.2.	Klientų informavimas (jei yra galimybė) apie galimus paslaugų teikimo sutrikimus ir numatomą sutrikimų pašalinimo terminą	Nedelsiant, bet ne vėliau kaip per 15 min.	Valdymo grupė
		3.3.	Padarytos žalos įvertinimas ir priemonių plano parengimas	Per 1,5 val. nuo incidento nustatymo	Valdymo grupė Atkūrimo grupė
		3.4.	Padarytos žalos likvidavimas	Priklausomai nuo atkūrimo darbų apimties – nuo 3 d. d. iki 2 mėn.	Atkūrimo grupė
4.	Gamtos veiksniai (potvynis, uraganas, oro ir kt. pavojus)	4.1.	Klientų ir darbuotojų informavimas (jei yra galimybė) apie galimus paslaugų teikimo sutrikimus ir numatomą sutrikimų pašalinimo terminą	Nedelsiant, bet ne vėliau kaip per 15 min.	Valdymo grupė
		4.2.	Padarytos žalos įvertinimas	Per 15 min. nuo incidento nustatymo	Valdymo grupė Atkūrimo grupė

		4.3.	Priemonių plano padarytai žalai likviduoti sudarymas	Per 30 min. nuo incidento nustatymo	Valdymo grupė Atkūrimo grupė
		4.4.	Padarytos žalos likvidavimas	Priklausomai nuo atkūrimo darbų apimties – nuo 3 d. d. iki 2 mėn.	Atkūrimo grupė
5.	Gaisras	5.1.	Priešgaisrinės gelbėjimo tarnybos rekomendacijų vykdymas	Pagal Priešgaisrinės gelbėjimo tarnybos rekomendacijas	Valdymo grupės vadovas
		5.2.	Darbuotojų informavimas apie evakavimą	Nedelsiant	Valdymo grupė
		5.3.	Klientų informavimas (jei yra galimybė) apie galimus paslaugų teikimo sutrikimus ir numatomą sutrikimų pašalinimo terminą	Nedelsiant, bet ne vėliau kaip per 15 min.	Valdymo grupė
		5.4.	Padarytos žalos įvertinimas ir priemonių plano sudarymas	Esant galimybei ne vėliau kaip per 2 d. d.	Valdymo grupė Atkūrimo grupė
		5.5.	Padarytos žalos likvidavimas	Priklausomai nuo atkūrimo darbų apimties – nuo 3 d. d. iki 2 mėn.	Atkūrimo grupė
6.	Programinės įrangos sugadinimas, praradimas	6.1.	Teisėsaugos institucijos informavimas ir jų nurodymų vykdymas	Nedelsiant	Valdymo grupės vadovas
		6.2.	Padarytos žalos įvertinimas ir priemonių plano sudarymas	Per 1 d. d. nuo incidento nustatymo	Valdymo grupė Atkūrimo grupė
		6.3.	Padarytos žalos likvidavimas	Priklausomai nuo atkūrimo darbų apimties – nuo 3 d. d. iki 2 mėn.	Atkūrimo grupė
7.	Pagrindinių tarnybinių stočių	7.1.	Teisėsaugos institucijos nurodymų vykdymas	Nedelsiant	Valdymo grupės vadovas

	sugadinimas ir (ar) praradimas	7.2.	Padarytos žalos įvertinimas ir priemonių plano sudarymas	Per 1 d. d. nuo incidento nustatymo	Valdymo grupė Atkūrimo grupė
		7.3.	Padarytos žalos likvidavimas	Priklausomai nuo atkūrimo darbų apimties – nuo 3 d. d. iki 2 mėn.	Atkūrimo grupė

Papildyta priedu:
Nr. V-286, 2021-04-22, paskelbta TAR 2021-04-22, i. k. 2021-08376
Pakeistas priedo pavadinimas:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436

Saugiojo tinklo veiklos
tęstinumo plano
2 priedas

SAUGIOJO TINKLO VEIKLOS TĘSTINUMO PLANO VEIKSMINGUMO IŠBANDYMO METU PASTEBĖTŲ TRŪKUMŲ ATASKAITA

Valdymo grupės vadovas:

Valdymo grupės nariai:

Plano veiksmingumo išbandymo data ir būdas:

Plano veiksmingumo išbandymo scenarijus:
(trumpas aprašymas)

Plano veiksmingumo išbandymo metu pastebėti trūkumai:

Eil. Nr.	**Trūkumas**	**Siūlomas sprendimas trūkumui šalinti / pastaba**

_____ _____

(Valdymo grupės vadovo vardas ir pavardė) (parašas)

Papildyta priedu:

Nr. V-286, 2021-04-22, paskelbta TAR 2021-04-22, i. k. 2021-08376

3 priedas. *Neteko galios nuo 2023-02-04*
Priedo naikinimas:
Nr. V-94, 2023-02-03, paskelbta TAR 2023-02-03, i. k. 2023-02047

4 priedas. *Neteko galios nuo 2022-09-24*
Priedo naikinimas:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436
Papildyta priedu:
Nr. V-286, 2021-04-22, paskelbta TAR 2021-04-22, i. k. 2021-08376

PATVIRTINTA
Lietuvos Respublikos
krašto apsaugos ministro
2021 m. gegužės 11 d.
įsakymu Nr. V-338

SAUGIOJO TINKLO INCIDENTŲ, POKYČIŲ IR PROBLEMŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
VALDYMO PROCESŲ RYŠYS SU KITAIS PASLAUGŲ VALDYMO PROCESAIS

PIRMASIS SKIRSNIS
INCIDENTŲ VALDYMO PROCESŲ RYŠYS SU KITAIS PASLAUGŲ VALDYMO PROCESAIS

1. Incidentų valdymo procesas susijęs su problemų valdymo procesu, jei yra aptinkama pasikartojančių incidentų.

2. Incidentų valdymo procesas susijęs su pokyčių valdymo procesu, jei sprendžiant incidentą reikia atlikti paslaugai teikti naudojamų išteklių keitimus.

3. Incidentų valdymo procesas susijęs su sąrankos valdymo procesu, fiksuojant įrangos nustatymus, kurie sukėlė incidentą.

4. Problemų, pokyčių, sąrankos valdymo procesų dalyviams pateikiama ši informacija, sukaupta incidentų valdymo proceso metu:

Informacija	Valdymo procesas
Incidento priežastis, sprendimo būdas, informacija apie sugedusią įrangą	Problemų valdymas Pokyčių valdymas Sąrankos valdymas
Incidentų kiekis vienai paslaugai ir (ar) naudotojui per ataskaitinį laikotarpį	Problemų valdymas

ANTRASIS SKIRSNIS
POKYČIŲ VALDYMO PROCESŲ RYŠYS SU KITAIS PASLAUGŲ VALDYMO PROCESAIS

5. Pokyčių valdymo procesas susijęs su incidentų valdymo procesu, kai sprendžiant incidentą reikia atlikti paslaugai teikti reikalingų išteklių keitimą.

6. Pokyčių valdymo procesas susijęs su sąrankos valdymo procesu, kai sprendžiant incidentą ar problemą keičiami su Saugiojo tinklo paslaugomis susijusių išteklių duomenys, nustatymai.

7. Pokyčių valdymo procesas susijęs su problemų valdymo procesu, kai sprendžiant problemą būtina atlikti Saugiojo tinklo paslaugoms teikti reikalingų išteklių keitimą.

8. Incidentų, problemų, sąrankos valdymo procesų dalyviams pateikiama ši informacija, sukaupta pokyčių valdymo proceso metu:

Informacija	Valdymo procesas

Saugiojo tinklo naudotojų duomenys: pavadinimas, buveinės ir (arba) struktūrinio (-ių) padalinio (-ių), kuriame yra įrengta prieiga prie Saugiojo tinklo, adresas	Sąrankos valdymas Incidentų valdymas Problemų valdymas
Keičiamos įrangos duomenys (tipas, pavadinimas, inventorinis numeris)	Sąrankos valdymas Incidentų valdymas Problemų valdymas
Vykdomo pokyčio duomenys (statusas, įvykdymo data, keitimo rezultatai)	Incidentų valdymas Problemų valdymas

TREČIASIS SKIRSNIS
PROBLEMŲ VALDYMO PROCESŲ RYŠYS SU KITAIS PASLAUGŲ VALDYMO PROCESAIS

9. Problemų valdymo procesas susijęs su incidentų valdymo procesu, kuriam svarbu incidentų kiekis vienai paslaugai, nuolat besikartojantys incidentai, tarpusavyje susiję incidentai, kuriems nustatyta ta pati klaidos sukėlimo priežastis.

10. Problemų valdymo procesas susijęs su keitimų valdymo procesu, jei sprendžiant problemą reikia atlikti paslaugai teikti naudojamų išteklių keitimus. Pokyčių valdymo procese priimant sprendimus dėl išteklių keitimo naudojami duomenys apie paslaugai teikti reikalingų išteklių pasikartojančius gedimus.

11. Problemų valdymo procesas susijęs su sąrankos valdymo procesu, fiksuojant įrangos nustatymus, kurie sukėlė pasikartojančius gedimus.

12. Incidentų, pokyčių, sąrankos valdymo procesų dalyviams pateikiama ši informacija, sukaupta problemų valdymo proceso metu:

Informacija	Valdymo procesas
Besikartojantys incidentai vienai paslaugai, besikartojančių incidentų priežastys, informacija apie sugedusią įrangą	Incidentų valdymas Pokyčių valdymas Sąrankos valdymas
Laikinas problemos sprendimas	
Nuolatinis problemos sprendimas	

II SKYRIUS
VALDYMO PROCESO DALYVIAI

PIRMASIS SKIRSNIS
INCIDENTŲ VALDYMO PROCESO DALYVIAI

13. Incidentų valdymo proceso dalyviai:

13.1. Aptarnavimo ir paslaugų valdymo skyriaus darbuotojas;

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

13.2. Tinklo technologijų departamento darbuotojas, vykdantis pasyvų budėjimą ne darbo vietoje, pasibaigus darbo dienai, taip pat poilsio ir švenčių dienomis ir pasirengęs reaguoti į incidentus (toliau – Budėtojas);

13.3. Tinklo technologijų departamento incidentų sprendimo grupė arba darbuotojas;

13.4. Informacinių technologijų skyriaus incidentų sprendimo grupė arba darbuotojas;

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

13.5. Saugumo skyriaus incidentų sprendimo grupė arba darbuotojas;

13.6. Aptarnavimo ir paslaugų valdymo skyriaus darbuotojas, atsakingas už matavimo rodiklių kaupimą, analizę ir teikimą.

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

14. Incidentų valdymo proceso dalyvių atliekamos pagrindinės funkcijos:

Proceso dalyviai	Incidento registravimas ir perdavimas sprendimui priimti	Incidento sprendimas	Incidento priskyrimas trečiosioms šalims	Incidento išsprendimas ir uždarymas	Incidentų rodiklių kaupimas, analizė ir teikimas
Aptarnavimo ir paslaugų valdymo skyriaus darbuotojas / Budėtojas	Atlieka	Atlieka		Atlieka	
Incidentų sprendimo grupė arba darbuotojas		Atlieka	Atlieka	Atlieka	
Trečiosios šalys		Atlieka			
Už matavimo rodiklių kaupimą, analizę ir teikimą atsakingas asmuo					Atlieka

Punkto pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

ANTRASIS SKIRSNIS
POKYČIŲ VALDYMO PROCESO DALYVIAI

15. Pokyčių valdymo procese dalyvauja:

15.1. Aptarnavimo ir paslaugų valdymo skyriaus darbuotojas;

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

15.2. incidentą sprendusi grupė arba darbuotojas;

15.3. problemą sprendusi grupė arba darbuotojas;

15.4. darbuotojas, kuriam pavesta atlikti Saugiojo tinklo įrangos keitimo / atnaujinimo darbus;

15.5. Kertinio valstybės telekomunikacijų centro (toliau – KVTC) direktoriaus sudaryta pokyčių vertinimo grupė;

15.6. KVTC direktoriaus sudarytas pokyčių tvirtinimo komitetas;

Proceso dalyviai	Pokyčio registra-vimas	Pokyčio vertini-mas	Pokyčio tvirti-nimas	Pokyčio vykdymas	Pokyčio patikrinimas ir uždarymas	Matavimo rodiklių kaupimas, analizė ir teikimas
Aptarnavimo paslaugų valdymo skyriaus darbuotojas	Atlieka					
Incidentą / problemą sprendusi grupė arba darbuotojas	Atlieka					
KVTC darbuotojas, atsakingas už įrangos keitimą / atnaujinimą	Atlieka					
Pokyčių vertinimo grupė		Atlieka				
Pokyčių tvirtinimo komitetas			Atlieka			
KVTC direktorius			Atlieka			
Pokyčių vykdymo grupė arba darbuotojas				Atlieka	Atlieka	
Už matavimo rodiklių kaupimą, analizę ir teikimą atsakingas asmuo						Atlieka

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

15.7. pokyčių vykdymo grupė arba darbuotojas;

15.8. KVTC direktorius;

15.9. Aptarnavimo ir paslaugų valdymo skyriaus darbuotojas, atsakingas už matavimo rodiklių kaupimą, analizę ir teikimą.

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

16. Pokyčių valdymo proceso dalyvių atliekamos pagrindinės funkcijos:

TREČIASIS SKIRSNIS
PROBLEMŲ VALDYMO PROCESO DALYVIAI

17. Problemų valdymo proceso dalyviai:

17.1. Aptarnavimo ir paslaugų valdymo skyriaus darbuotojas;

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

17.2. incidentų sprendimo grupė arba darbuotojas;

17.3. darbuotojas, atsakingas už problemos sprendimą;

17.4. Aptarnavimo ir paslaugų valdymo skyriaus darbuotojas, atsakingas už matavimo rodiklių kaupimą, analizę ir teikimą.

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

18. Problemų valdymo proceso dalyviai ir jų atliekamos pagrindinės funkcijos:

Proceso dalyviai	Problemos registravimas ir vertinimas	Problemos tyrimas ir priskyrimas atsakingam asmeniui	Problemos sprendimas	Problemos perdavimas trečiosioms šalims	Išspręstos problemos stebėjimas	Problemos uždarymas	Matavimo rodiklių kaupimas ir analizė
Aptarnavimo ir paslaugų valdymo skyriaus darbuotojas	Atlieka				Atlieka	Atlieka	
Incidentų sprendimo grupė arba darbuotojas		Atlieka					
Darbuotojas, atsakingas už problemos sprendimą			Atlieka	Atlieka			
Trečiosios šalys			Atlieka				
Už matavimo rodiklių kaupimą, analizę ir teikimą atsakingas asmuo							Atlieka

Punkto pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

III SKYRIUS
BŪSENOS

PIRMASIS SKIRSNIS
INCIDENTŲ BŪSENOS

19. Naudojamos šios incidentų valdymo esminių etapų būsenos:

Būsena	Aprašymas

Būsena	Aprašymas
Užregistruota	Sukurta incidento kortelė
Priskirta	Priskirta incidento sprendimo grupė arba darbuotojas
Sprendžiama	Incidento sprendimo grupė arba darbuotojas pradėjo incidento sprendimo veiksmus
Laukiama	Laukiama papildomos informacijos arba veiksmų iš naudotojo arba suderintas incidento sprendimo laikas
Sprendžiama trečiosios šalies	Incidento sprendimas perduotas vykdyti trečiosioms šalims
Grąžinta spręsti	Incidentas grąžintas spręsti anksčiau incidentą sprendusiai grupei arba darbuotojui
Išspręsta	Incidentas išspręstas
Uždaryta	Incidentas uždarytas (nebegalimas pakartotinis atidarymas, šalinimo veiksmų pratęsimas)

ANTRASIS SKIRSNIS
POKYČIŲ BŪSENOS

20. Naudojamos šios pokyčių valdymo esminių etapų būsenos:

Statusas	Aprašymas
Užregistruota	Sukurta pokyčio kortelė
Vertinama	Pokytis perduotas vertinti pokyčių vertinimo grupei
Tvirtinama	Pokytis perduotas tvirtinti pokyčių tvirtinimo komitetui
Atmesta	Pokytis grąžintas vertinti ir (ar) tikslinti pokyčių vertinimo grupei

Statusas	Aprašymas
Vykdoma	Patvirtintas pokytis perduotas vykdyti pokyčių vykdymo grupei

Statusas	Aprašymas	
Užregistruota	Sukurta problemos kortelė, pateikta reikiama informacija	
Priskirta	Perduota tirti problemą incidentų sprendimo grupei	
Tiriama	Analizuojama problema, nustatoma pagrindinė priežastis, paskiriamas už problemos sprendimą atsakingas asmuo, nustatomas problemos sprendimo terminas	
Sprendžiama	Už problemos sprendimą atsakingas asmuo vykdo laikino problemos sprendimo ir (ar) nuolatinio sprendimo diegimo darbus	
Sprendžiama trečiosios šalies	Problemos sprendimas perduotas vykdyti trečiosioms šalims, vykdoma pokyčių trečiųjų šalių sprendimo priežiūra	Pokytis įvykdytas
Išspręsta	Įdiegtas problemos laikinas ar nuolatinis sprendimas	
Stebima	Vykdomas išspręstos problemos stebėjimas	
Grąžinta spręsti	Problema grąžinta spręsti anksčiau problemą sprendusiam asmeniui	
Uždaryta	Problema išspręsta	
Atlikta		
Uždaryta		Pokytis uždarytas

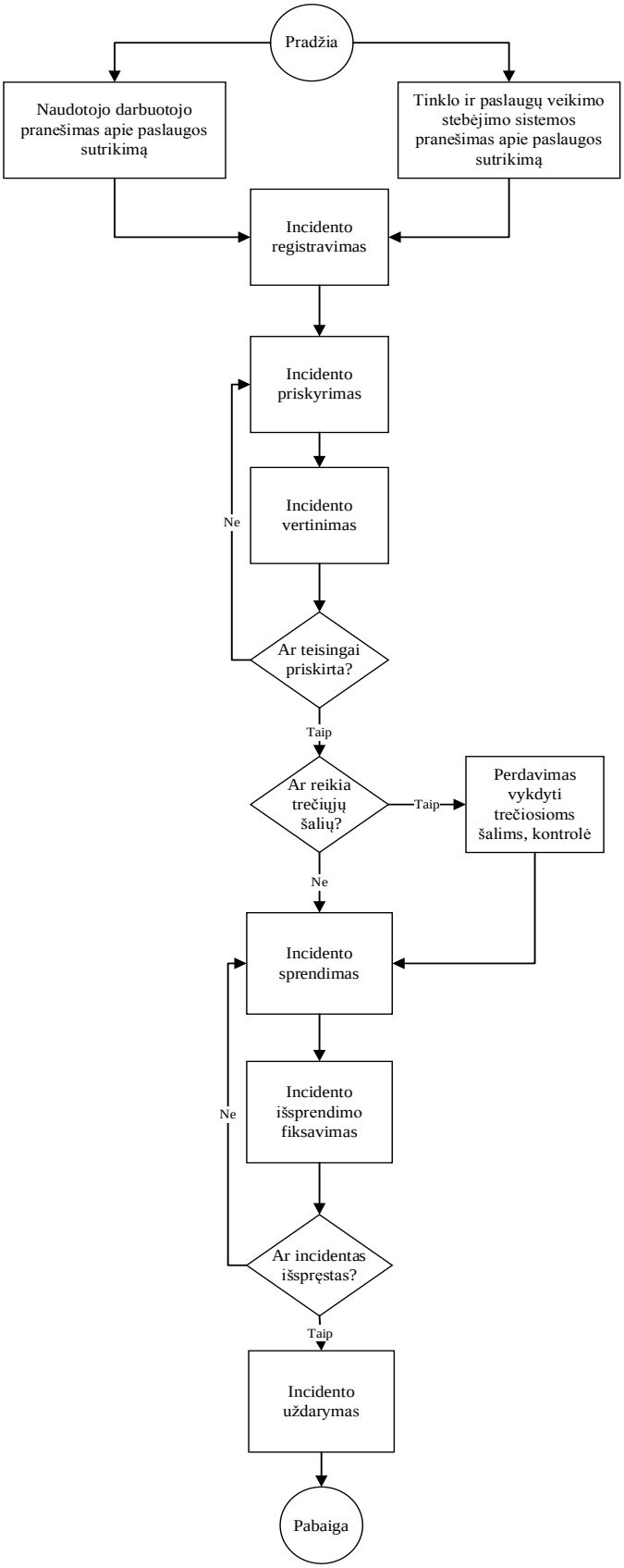
TREČIASIS SKIRSNIS
PROBLEMŲ BŪSENOS

21. Naudojamos šios problemų valdymo esminių etapų būsenos:

IV SKYRIUS
VALDYMO PROCESO SCHEMA IR PROCESO ĮGYVENDINIMO METU ATLIEKAMI VEIKSMAI

PIRMASIS SKIRSNIS
INCIDENTŲ VALDYMO PROCESO SCHEMA IR PROCESO ĮGYVENDINIMO METU ATLIEKAMI VEIKSMAI

22. Incidentų valdymo proceso schema:


Pradžia
Naudotojo darbuotojo pranešimas apie paslaugos sutrikimą
Tinklo ir paslaugų veikimo stebėjimo sistemos pranešimas apie paslaugos sutrikimą
Incidento registravimas
Incidento priskyrimas
Incidento vertinimas
Ne
Ar teisingai priskirta?
Taip
Ar reikia trečiųjų šalių?
Taip
Perdavimas vykdyti trečiosioms šalims, kontrolė
Ne
Incidento sprendimas
Incidento išsprendimo fiksavimas
Ne
Ar incidentas išspręstas?
Taip
Incidento uždarymas
Pabaiga

23. Incidento registravimas:

23.1. paslaugų valdymo priemonės naudotojas dėl paslaugos sutrikimo, informacijos saugumo incidento kreipiasi registruodamas įvykį paslaugų valdymo priemonėje;

23.2. kiti Saugiojo tinklo naudotojo darbuotojai apie incidentą gali pranešti telefonu 8 5 239 1727 arba el. paštu pagalba@kvtc.gov.lt;

23.3. galimus incidentus taip pat fiksuoja Saugiojo tinklo paslaugų teikimo stebėjimo priemonė ir automatiškai išsiunčia pranešimą 23.2 papunktyje nurodytu el. paštu;

23.4. Aptarnavimo ir paslaugų valdymo skyriaus darbuotojas arba Budėtojas (ne darbo metu) (toliau – Atsakingas asmuo), telefonu gavęs pranešimą apie incidentą, užregistruoja jį paslaugų valdymo priemonėje;

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

23.5. visi incidentai privalo būti užregistruoti paslaugų valdymo priemonėje;

23.6. registruojant incidento kortelėje nurodoma ši informacija:

23.6.1. Saugiojo tinklo naudotojo pavadinimas;

23.6.2. Saugiojo tinklo naudotojui teikiama paslauga, kurios teikimas sutriko;

23.6.3. Saugiojo tinklo naudotojo darbuotojo pateikta informacija apie incidentą, jo pasireiškimo aplinkybes ir pan.;

23.6.4. incidento poveikio lygis;

23.6.5. incidento svarbos lygis;

23.6.6. incidento prioriteto lygis, nustatomas automatiškai atsižvelgiant į incidento poveikio lygį ir incidento svarbos lygį.

24. Incidento priskyrimas:

24.1. Atsakingas asmuo atlieka pirminį incidento vertinimą;

24.2. nustatęs, kad incidentas gali būti susijęs su informacijos ar kibernetiniu saugumu, perduoda jį spręsti Saugumo skyriaus incidentų sprendimo grupei arba darbuotojui;

24.3. nustatęs, kad incidentas susijęs su Saugiojo tinklo veikla, perduoda jį spręsti Tinklo technologijų departamento arba Informacinių technologijų skyriaus incidentų sprendimo grupei arba darbuotojui.

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

25. Incidento sprendimas:

25.1. Saugumo skyriaus incidentų sprendimo grupė arba darbuotojas, gavę priskirtą incidentą, įvertina jį ir:

25.1.1. jei incidentas susijęs su informacijos ar kibernetiniu saugumu, sprendžia jį vadovaudamiesi Saugiojo tinklo valdytojo nustatyta tvarka;

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

25.1.2. esant poreikiui, pakeičia incidento poveikio, svarbos ir prioriteto lygį paslaugų valdymo priemonėje;

25.1.3. jei incidentas nėra susijęs su informacijos ar kibernetiniu saugumu, grąžina jį paslaugų valdymo priemonėmis Atsakingam asmeniui;

25.2. Tinklo technologijų departamento ar Informacinių technologijų departamento incidentų sprendimo grupė arba darbuotojai, gavę jiems priskirtą incidentą, įvertina jį ir:

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

25.2.1. jei incidentas susijęs su Saugiojo tinklo veikla, sprendžia jį;

25.2.2. esant poreikiui, pakeičia incidento poveikio, svarbos ir prioriteto lygį paslaugų valdymo priemonėje;

25.2.3. jei nustato, kad incidentui spręsti reikia trečiųjų šalių veiksmų, perduoda vykdymą trečiosioms šalims, kontroliuoja incidento sprendimą;

25.2.4. jei incidentas nėra susijęs su Saugiojo tinklo veikla, grąžina jį paslaugų valdymo priemonėmis Atsakingam asmeniui.

26. Incidento išsprendimas ir uždarymas:

26.1. incidentą išsprendusi incidentų sprendimo grupė arba darbuotojas paslaugų valdymo priemonėje pažymi, kad incidentas išspręstas, nurodo jo kilimo priežastį bei sprendimo būdą;

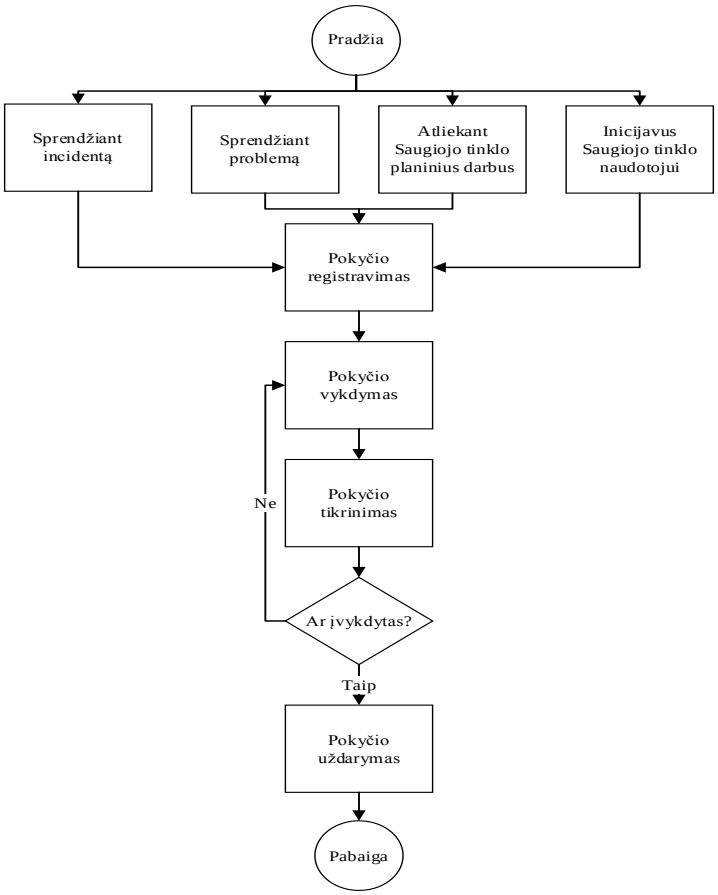
26.2. jei naudotojo darbuotojas informuoja, kad incidentas nėra pašalintas, Atsakingas asmuo grąžina jį spręsti anksčiau incidentą sprendusiai grupei arba darbuotojui;

26.3. incidentas uždaromas gavus apie incidentą pranešusio naudotojo patvirtinimą, kad incidentas išspręstas, arba automatiškai po 24 val.

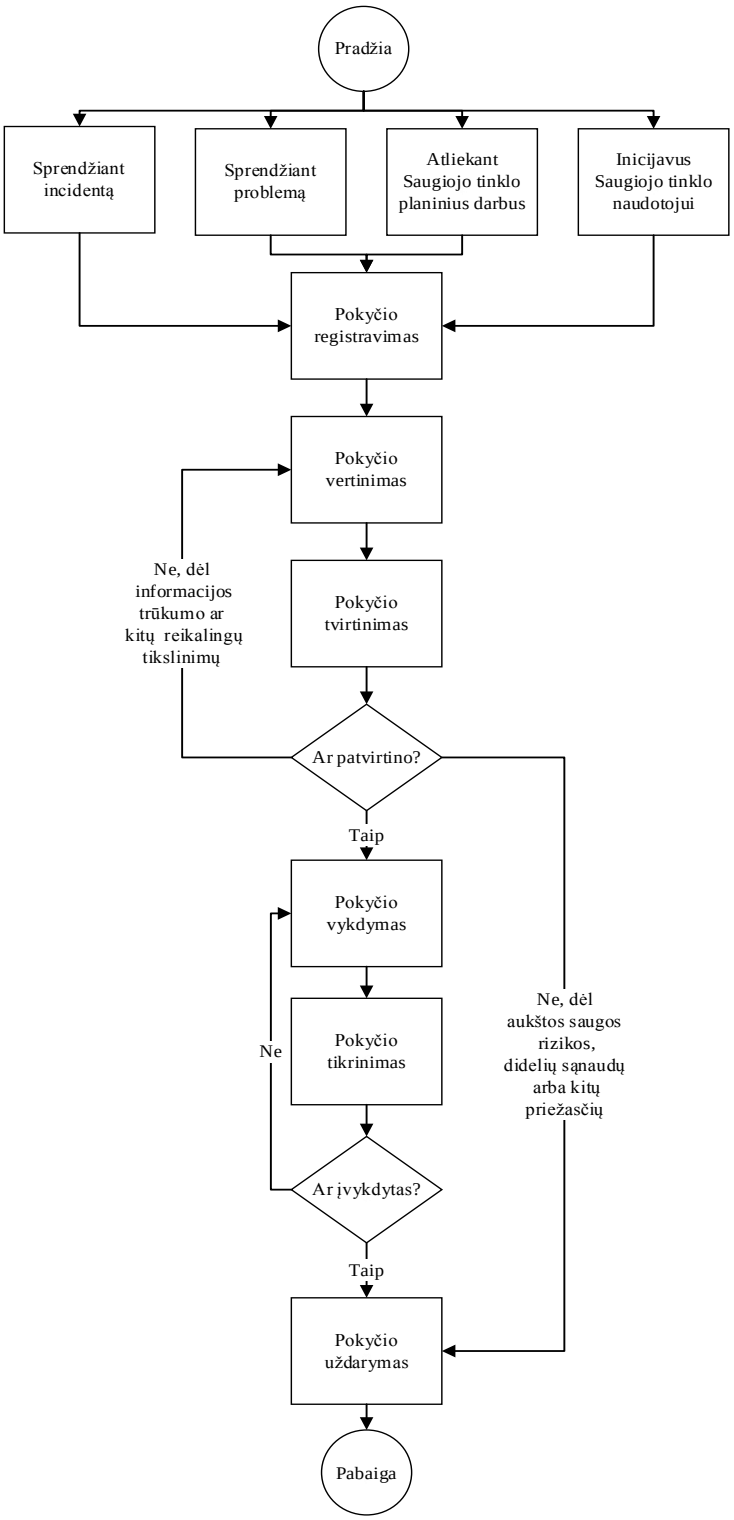
ANTRASIS SKIRSNIS
POKYČIŲ VALDYMO PROCESO SCHEMA IR PROCESO ĮGYVENDINIMO METU ATLIEKAMI VEIKSMAI

27. Pokyčių valdymo schemos:

27.1. standartinio pokyčio schema



27.2. nestandartinio pokyčio schema:



28. Pokyčio registravimas:

28.1. sprendžiant incidentą pokytį registruoja jį sprendusi incidento sprendimo grupė arba darbuotojas;

28.2. sprendžiant problemą pokytį registruoja ją sprendusi problemų sprendimo grupė arba darbuotojas;

28.3. vykdant planinius įrangos keitimo / atnaujinimo darbus, pokytį registruoja už įrangos pakeitimą / atnaujinimą paskirtas atsakingas darbuotojas;

28.4. paslaugų valdymo priemonės naudotojas pokytį inicijuoja paslaugų valdymo priemonėje;

28.5. kiti Saugiojo tinklo naudotojo darbuotojai pokytį inicijuoja raštu arba elektroniniu paštu paslaugos@kvtc.gov.lt, šiuos pokyčius paslaugų valdymo priemonėje užregistruoja Aptarnavimo ir paslaugų valdymo skyriaus darbuotojai;

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

28.6. visi pokyčiai privalo būti užregistruoti paslaugų valdymo priemonėje.

28.7. registruojant pokyčio kortelėje nurodoma ši informacija:

28.7.1. Saugiojo tinklo naudotojo duomenys: pavadinimas, buveinės ir (arba) struktūrinio (-ių) padalinio (-ių), kuriame yra įrengta prieiga prie Saugiojo tinklo, adresas, Saugiojo tinklo naudotojo darbuotojo kontaktinė informacija;

28.7.2. jei sprendžiamas incidentas arba problema – jų numeris;

28.7.3. Saugiojo tinklo paslauga arba Saugiojo tinklo išteklius, kurio pokytis vykdomas;

28.7.4. pokyčio priežastis ir detalus aprašymas;

28.7.5. pokyčio prioritetas ir įvykdymo terminas;

28.7.6. už pokyčio vertinimą atsakinga pokyčio vertinimo grupė.

29. Pokyčio vertinimą atlieka:

29.1. jei pokytis standartinis, jo vertinimo procedūra atlikta iš anksto už konkrečios paslaugos teikimą atsakingos pokyčių vertinimo grupės;

29.2. jei pokytis nestandartinis, jį vertina už konkrečios paslaugos teikimą atsakinga pokyčių vertinimo grupė;

29.3. esant poreikiui, pokyčio vertinimo grupė perduoda pokyčio vertinimą atlikti trečiosioms šalims.

30. Pokytį tvirtina:

30.1. jei pokytis standartinis, jo tvirtinimo procedūra atlikta iš anksto pokyčių tvirtinimo komiteto;

30.2. jei pokytis nestandartinis, jį tvirtina pokyčių tvirtinimo komitetas;

30.3. jei pokytis skubus, jį tvirtina KVTC direktorius savo sprendimu el. paštu, telefonu ar kitomis priemonėmis, vėliau tai pažymima paslaugų valdymo priemonėje;

30.4. jei pokytis patvirtinamas, jis perduodamas vykdyti pokyčių vykdymo grupei arba darbuotojui;

30.5. jei pokytis atmetamas dėl informacijos trūkumo ar kitų reikalingų tikslinimų, jis grąžinamas vertinti ir (ar) tikslinti iš naujo;

30.6. jei pokytis atmetamas dėl per aukštos saugos rizikos, didelių sąnaudų ar yra nepriimtinas dėl kitų priežasčių, netinkamai pagrįstas, jis uždaromas, nurodant uždarymo priežastis;

30.7. nepatvirtinti pokyčiai negali būti vykdomi.

31. Pokyčio vykdymas:

31.1. pokytį vykdo pokyčių vykdymo grupė, kuri gali būti nuolatinė arba sudaroma kiekvienam pokyčiui vykdyti, arba darbuotojas.

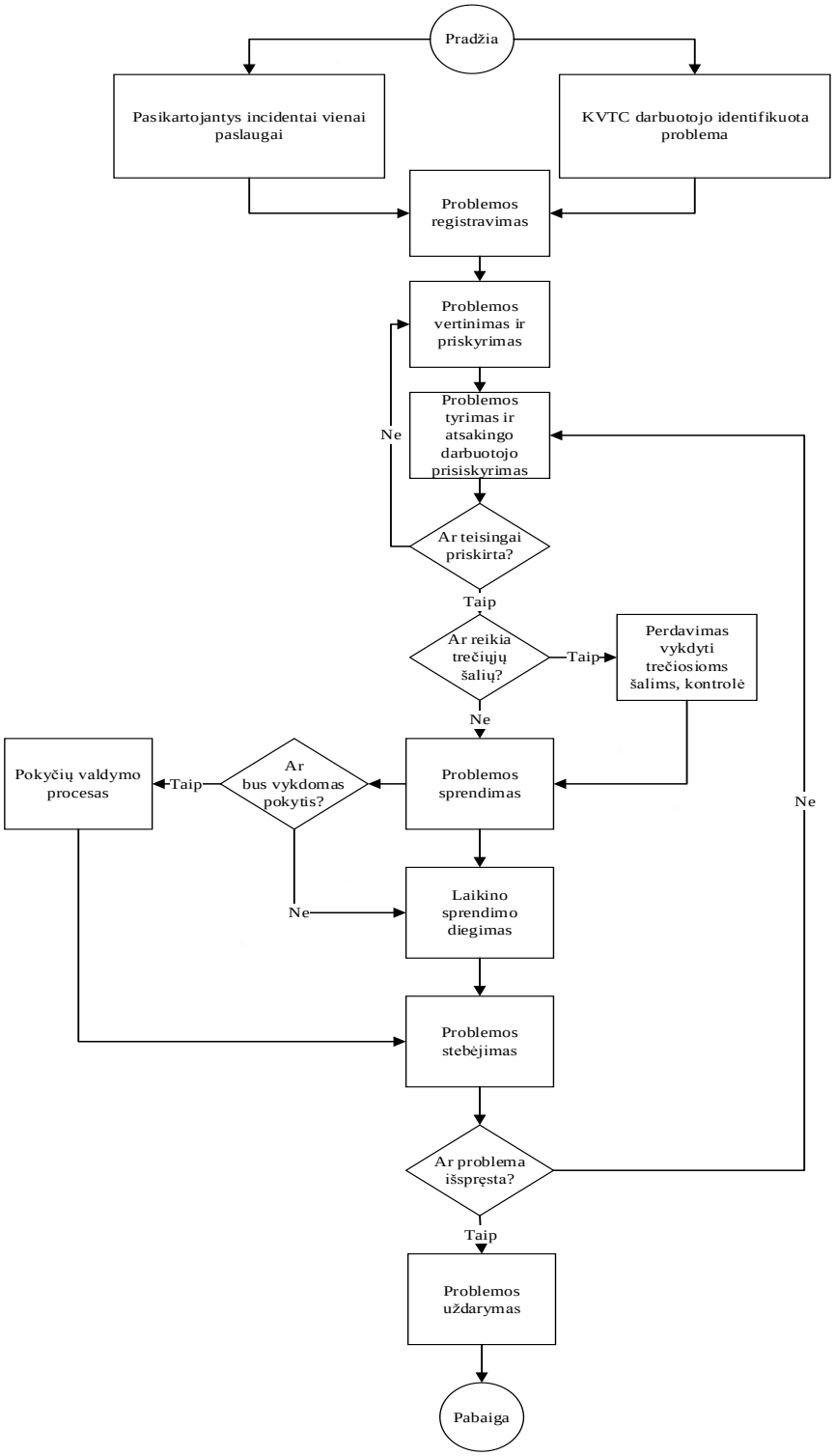
32. Pokyčio tikrinimas ir uždarymas:

32.1. pokytį įvykdžiusi pokyčio vykdymo grupė arba darbuotojas patikrina, ar pokytis įvykdytas, ir gavę pokytį inicijavusio asmens patvirtinimą uždaro jį;

32.2. jei pokytį inicijavęs asmuo informuoja, kad pokytis įvykdytas nesėkmingai, pokytis grąžinimas vykdyti pokyčio vykdymo grupei arba darbuotojui.

TREČIASIS SKIRSNIS
PROBLEMŲ VALDYMO PROCESO SCHEMA IR PROCESO ĮGYVENDINIMO METU ATLIEKAMI VEIKSMAI

33. Problemų valdymo proceso schema:



34. Problemos registravimas ir vertinimas:

34.1. Aptarnavimo ir paslaugų valdymo skyriaus darbuotojas, nustatęs, kad incidentas kartojasi, registruoja problemą dėl pasikartojančių incidentų vienai paslaugai paslaugų valdymo priemonėje;

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

34.2. jei problemą nustato Tinklo technologijų departamento, Informacinių technologijų skyriaus arba Saugumo skyriaus darbuotojai, jos aprašymą el. paštu persiunčia Aptarnavimo ir paslaugų valdymo skyriaus darbuotojui;

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

34.3. Aptarnavimo ir paslaugų valdymo skyriaus darbuotojas, gavęs el. laišką su problemos aprašymu, užregistruoja ją paslaugų valdymo priemonėje;

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

34.4. visos problemos privalo būti užregistruotos paslaugų valdymo priemonėje;

34.5. registruojant problemą, nurodoma ši informacija:

34.5.1. Saugiojo tinklo naudotojo, kuriam kartojasi incidentai, pavadinimas;

34.5.2. paslauga, kuriai kartojasi incidentai;

34.5.3. pasikartojantys incidentai, jų aprašymai ir gedimo priežastys;

34.5.4. problemos tyrimo terminas;

34.5.5. problemos poveikio lygis;

34.5.6. problemos svarbos lygis;

34.5.7. problemos prioritetas, kuris nustatomas automatiškai atsižvelgiant į problemos poveikio lygį ir problemos svarbos lygį;

34.6. Aptarnavimo ir paslaugų valdymo skyriaus darbuotojas atlieka pirminį problemos vertinimą;

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

34.7. nustatęs, kad problema gali būti susijusi su informacijos ar kibernetiniu saugumu, perduoda ją spręsti Saugumo skyriaus incidentų sprendimų grupei arba darbuotojui;

34.8. nustatęs, kad problema susijusi su Saugiojo tinklo veikla, perduoda ją spręsti Tinklo technologijų departamento arba Informacinių technologijų skyriaus incidentų sprendimų grupei arba darbuotojui.

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

35. Problemos tyrimas ir priskyrimas:

35.1. Saugumo skyriaus incidentų sprendimo grupė arba darbuotojas, gavę priskirtą problemą, tiria ją ir:

35.1.1. jei problema susijusi su informacijos ar kibernetiniu saugumu, priskiria už problemos sprendimą atsakingą darbuotoją ir nustato problemos sprendimo terminą;

35.1.2. esant poreikiui, pratęsia problemos tyrimo terminą;

35.1.3. jei problema nėra susijusi su informacijos ar kibernetiniu saugumu, grąžina ją paslaugų valdymo priemonėmis Aptarnavimo ir paslaugų valdymo skyriaus darbuotojui;

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

35.2. Tinklo technologijų departamento ar Informacinių technologijų departamento incidentų sprendimo grupė arba darbuotojas, gavę priskirtą problemą, tiria ją ir:

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

35.2.1. jei problema susijusi su Saugiojo tinklo veikla, priskiria už problemos sprendimą atsakingą darbuotoją ir nustato problemos sprendimo terminą;

35.2.2. esant poreikiui, pratęsia problemos tyrimo terminą;

35.2.3. jei problema nėra susijusi su Saugiojo tinklo veikla, grąžina ją paslaugų valdymo priemonėmis Aptarnavimo ir paslaugų valdymo skyriaus darbuotojui.

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

36. Problemos sprendimas:

36.1. už problemos sprendimą atsakingas darbuotojas, esant poreikiui, gali pasitelkti kitus darbuotojus problemai spręsti;

36.2. jei nustatoma, kad problemai spręsti reikia trečiųjų šalių veiksmų, perduoda jos vykdymą trečiosioms šalims, kontroliuoja problemos sprendimą;

36.3. jei problemai pašalinti reikia atlikti paslaugų ar paslaugoms teikti naudojamų išteklių keitimus, užsakomas pokytis;

36.4. nustatyta problemos priežastis įrašoma paslaugų valdymo priemonėje;

36.5. nustatomas problemos sprendimas, jis vykdomas;

36.6. jei problemos sprendimas reikalauja didelių sąnaudų, gali sukelti riziką Saugiojo tinklo saugumui ar dėl kitų priežasčių yra netinkamas, įdiegiamas ir fiksuojamas laikinas problemos sprendimas.

37. Problemos stebėjimas ir uždarymas:

37.1. atlikus problemos sprendimui reikalingą keitimą, paslaugų valdymo priemonėje pažymima, kad problema išspręsta;

37.2. Aptarnavimo ir paslaugų valdymo skyriaus darbuotojas nustato ne trumpesnį nei dviejų savaičių stebėjimo laikotarpį, per kurį įsitikinama, kad problemos priežastis iš tikrųjų buvo pašalinta ir nebekyla sutrikimų, susijusių su nustatyta problemos priežastimi bei sprendimo metu padarytais keitimais:

37.2.1. jei problemos stebėjimo laikotarpiu Aptarnavimo ir paslaugų valdymo skyriaus darbuotojas nustato, kad problema nebuvo išspręsta, grąžina ją spręsti anksčiau problemą sprendusiam darbuotojui;

37.2.2. jei per nustatytą sprendimo stebėjimo laikotarpį problema nesikartoja, Aptarnavimo ir paslaugų valdymo skyriaus darbuotojas problemą uždaro.

Papunkčio pakeitimai:
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655

V SKYRIUS
KATEGORIJŲ SĄRAŠAS

PIRMASIS SKIRSNIS
INCIDENTŲ KATEGORIJŲ SĄRAŠAS

38. Incidentų kategorijos yra skirstomos pagal teikiamas paslaugas ir atitinka Saugiojo tinklo teikiamų paslaugų pavadinimus:

Incidentų kategorija	Aprašymas
Duomenų perdavimo paslaugos	Paslaugos „Duomenų perdavimas tinklo naudotojams ir jų struktūriniams padaliniams“ incidentai
Prieiga prie viešųjų ryšių tinklų	Paslaugos „Prieiga prie viešųjų ryšių tinklų“ incidentai
Kibernetinis saugumas	Paslaugos „Kolektyvinė apsauga kibernetinio saugumo priemonėmis“ incidentai
Prieiga prie ES informacinių išteklių	Paslaugos „Sąveika su Europos Sąjungos ir jos valstybių narių institucijų valdomais informaciniais ištekliais“ incidentai
Valstybės valdomų e. ryšių tinklų sujungimas	Paslaugos „Valstybės valdomų elektroninių ryšių tinklų, kurie naudojami vykdant valstybines mobilizacines užduotis, dalių sujungimas“ incidentai

ANTRASIS SKIRSNIS
POKYČIŲ KATEGORIJŲ SĄRAŠAS

39. Pokyčių kategorijos skirstomos pagal pokyčio kilimo priežastį:

Pokyčio kategorija		Aprašymas
Standartinis pokytis		Į Saugiojo tinklo tvarkytojo patvirtintą standartinių pokyčių sąrašą įtrauktas pokytis, kurio vertinimo bei tvirtinimo procedūros atliktos iš anksto, ir kai išteklių sąnaudos ir rizikos žinomos
Nestandartinis pokytis	Skubus	Kai pokytis kyla sprendžiant incidentą arba problemą ir kai išteklių sąnaudos nėra iš anksto įvertintos ir suplanuotos
	Neskubus	Su vienkartiniais Saugiojo tinklo įrangos keitimo / atnaujinimo darbais susiję pokyčiai, kai kiekvieno pokyčio veiksmai ir ištekliai planuojami ir vertinimo bei tvirtinimo procedūros nėra atliktos iš anksto

TREČIASIS SKIRSNIS
PROBLEMŲ KATEGORIJŲ SĄRAŠAS

40. Problemų kategorijos yra skirstomos pagal teikiamas paslaugas ir atitinka Saugiojo tinklo teikiamų paslaugų pavadinimas:

Sutrikimų kategorija	Aprašymas
Duomenų perdavimo	Paslaugos „Duomenų perdavimas tinklo naudotojams ir jų struktūriniams

paslaugos	padaliniams“ problemos
Prieiga prie viešųjų ryšių tinklų	Paslaugos „Prieiga prie viešųjų ryšių tinklų“ problemos
Kibernetinis saugumas	Paslaugos „Kolektyvinė apsauga kibernetinio saugumo priemonėmis“ problemos
Prieiga prie ES informacinių išteklių	Paslaugos „Sąveika su Europos Sąjungos ir jos valstybių narių institucijų valdomais informaciniais ištekliais“ problemos
Valstybės valdomų e. ryšių tinklų sujungimas	Paslaugos „Valstybės valdomų elektroninių ryšių tinklų, kurie naudojami vykdant valstybines mobilizacines užduotis, dalių sujungimas“ problemos

VI SKYRIUS
PRIORITETAI

PIRMASIS SKIRSNIS
INCIDENTŲ PRIORITETAI

41. Incidentų šalinimo prioriteto lygis nustatomas atsižvelgiant į incidento poveikio naudotojams lygį ir incidento skubumo lygį bei vertinamas balais nuo 5 (žemiausias) iki 1 (aukščiausias):

Poveikis	**Skubumas**		
	Žemas	**Vidutinis**	**Aukštas**
Iki 3 (trijų) naudotojų arba jų padalinių ir (ar) yra nedidelis (pvz., nedidelis kokybės pablogėjimas)	5	4	3
Daugiau kaip 3 (trims) naudotojams arba jų padaliniams	4	3	2
Daugiau kaip 9 (devyniems) naudotojams arba jų padaliniams	3	2	1

42. Incidentų skubumo lygiai:

42.1. aukštas, kai paslaugų teikimas visiškai nutrūksta;

42.2. vidutinis, kai paslaugos teikiamos, tačiau su tam tikrais sutrikimais;

42.3. žemas, kai paslaugos teikiamos, tačiau pablogėjo paslaugų kokybė.

43. Reakcijos į incidentus ir incidentų išsprendimo laikas nurodyti Prisijungimo prie Saugiojo valstybinio duomenų perdavimo tinklo, atsijungimo nuo jo ir elektroninių ryšių paslaugų teikimo šiuo tinklu tvarkos aprašo (Aprašas), patvirtinto Lietuvos Respublikos krašto apsaugos ministro 2019 m. liepos 2 d. įsakymu Nr. V-583 „Dėl Saugiojo tinklo veiklą užtikrinančių dokumentų patvirtinimo“, 1 priede.

44. Jei reakcijos į incidentus ir incidentų išsprendimo laikas nėra apibrėžtas Apraše, jis nustatomas pagal incidentų šalinimo prioriteto lygį:

Prioritetas	**Reakcijos laikas, val.**	**Išsprendimo laikas, val.**
1	0,5	8
2	1	8
3	1	12
4	1	24
5	2	48

ANTRASIS SKIRSNIS
POKYČIŲ PRIORITETAI

45. Pokyčio prioriteto lygis nustatomas atsižvelgiant į pokyčio kategoriją:

Pokyčio kategorija	Prioritetas
Pirma kategorija, kai pokytis vykdomas sprendžiant incidentą arba problemą	Aukštas
Antra kategorija, kai vykdomas paslaugų Saugiojo tinklo naudotojams diegimas, keitimas, nutraukimas	Vidutinis
Trečia kategorija, kai vykdomas planinis Saugiojo tinklo įrangos keitimas / atnaujinimas ir tai nesutrikdo Saugiojo tinklo paslaugų teikimo	Žemas

46. Pokyčių vykdymo laikai:

46.1. jei pokyčio prioritetas aukštas, jo vykdymo laikas negali viršyti incidento arba problemos sprendimo laiko, numatyto incidentų arba problemų valdymo procese;

46.2. jei pokyčio prioritetas vidutinis arba žemas, pokyčio vykdymo terminas negali viršyti pokyčio kortelėje nustatyto termino.

TREČIASIS SKIRSNIS
PROBLEMŲ PRIORITETAI

47. Problemų šalinimo prioriteto lygis nustatomas atsižvelgiant į problemos poveikio naudotojams lygį ir problemos skubumo lygį bei vertinamas balais nuo 5 (žemiausias) iki 1 (aukščiausias):

Poveikis	Skubumas		
	Žemas	Vidutinis	Aukštas
Iki 3 (trijų) naudotojų arba jų padalinių ir (ar) yra nedidelis (pavyzdžiui, nedidelis kokybės pablogėjimas)	5	4	3
Daugiau kaip 3 (trims) naudotojams arba jų padaliniams	4	3	2
Daugiau kaip 9 (devyniems) naudotojams arba jų padaliniams	3	2	1

48. Problemų skubumo lygiai:

48.1. aukštas, kai paslaugos visiškai neteikiamos;

48.2. vidutinis, kai paslaugos teikiamos su tam tikrais sutrikimais;

48.3. žemas, kai pablogėjusi paslaugų kokybė.

VII SKYRIUS
POŽYMIŲ SĄRAŠAS

PIRMASIS SKIRSNIS
INCIDENTŲ ŠALINIMO POŽYMIŲ SĄRAŠAS

49. Incidentai šalinami pagal šiuos požymius:

Požymis	Aprašymas
Įrangos gedimas	Nustačius įrangos gedimą, sprendžiama dėl jos taisymo arba keitimo
Konfigūracijos klaida	Nustačius konfigūracijos klaidą, pagal galimybes šalinama klaida arba kreipiamasi į trečiąsias šalis
Saugiojo tinklo naudotojų darbuotojų veiksmai	Nustačius Saugiojo tinklo naudotojų darbuotojų veiksmus, sukėlusius sutrikimą, sutrikimas šalinimas kartu su to darbuotojo pagalba
Trečiųjų šalių įtaka	Nustačius, kad sutrikimas sukeltas trečiųjų šalių veiksmų arba įvyko jų valdomoje infrastruktūroje, incidentas šalinamas su visų susijusių šalių pagalba

ANTRASIS SKIRSNIS
POKYČIŲ VYKDYMO POŽYMIŲ SĄRAŠAS

50. Pokyčiai vykdomi pagal šiuos požymius:

Požymis	Aprašymas
Pokytis, susijęs su incidentu arba problemos priežastimi	Sprendžiant incidentą arba problemą ir nustačius įrangos ar elektroninių ryšių tinklo gedimą, sprendžiama dėl jų taisymo arba keitimo
Pokytis, susijęs su Saugiojo tinklo naudotojo paslaugų užsakymu, keitimu, nutraukimu	Saugiojo tinklo naudotojo naujos paslaugos ar turimos paslaugos kiekybinių arba kokybinių parametrų keitimas, paslaugų nutraukimas
Pokytis, susijęs su planiniu Saugiojo tinklo išteklių keitimu	Pasenusios arba netinkamos naudoti įrangos pakeitimas

TREČIASIS SKIRSNIS
PROBLEMŲ ŠALINIMO POŽYMIŲ SĄRAŠAS

51. Problemos šalinamos pagal šiuos požymius:

Požymis	Aprašymas
Įrangos gedimas	Nustačius įrangos gedimą, sprendžiama dėl jos taisymo arba keitimo
Konfigūracijos klaida	Nustačius konfigūracijos klaidą, pagal galimybes šalinama klaida arba kreipiamasi į trečiąsias šalis
Naudotojų darbuotojų veiksmai	Nustačius naudotojų darbuotojų veiksmus, sukėlusius problemą, ji šalinama kartu su naudotojo darbuotojo pagalba

Trečiųjų šalių įtaka	Nustačius, kad problema kilo dėl trečiųjų šalių veiksmų arba įvyko jų valdomoje infrastruktūroje, problema šalinama su visų susijusių šalių pagalba

VIII SKYRIUS
VALDYMO PROCESO MATAVIMO RODIKLIAI

PIRMASIS SKIRSNIS
INCIDENTŲ VALDYMO PROCESO MATAVIMO RODIKLIAI

52. Incidentų valdymo proceso efektyvumui matuoti naudojami rodikliai:

52.1. incidentų, į kuriuos sureaguota laiku, dalis;

52.2. laiku išspręstų incidentų dalis;

52.3. grąžintų spręsti incidentų dalis.

53. 52 punkte nurodytų rodiklių siekiamos reikšmės:

Rodiklis	Siekiama reikšmė
Incidentų, į kuriuos sureaguota laiku, dalis	≥ 90 procentų
Laiku išspręstų incidentų dalis	≥ 90 procentų
Grąžintų spręsti incidentų dalis	≤ 10 procentų

54. Už matavimo rodiklių kaupimą, analizę ir jų teikimą atsakingas asmuo:

54.1. einamojo mėnesio pradžioje peržiūri praėjusio mėnesio užregistruotus ir spręstus incidentus;

54.2. skaičiuoja, ar 52 punkte nurodyti rodikliai atitinka 53 punkte pateiktas siekiamas šių rodiklių reikšmes;

54.3. rengia kiekvieno mėnesio incidentų rodiklių ataskaitą ir ją pateikia KVTC direktoriui;

54.4. ne rečiau kaip vieną kartą per ketvirtį organizuoja incidentų valdymo proceso bei jo efektyvumo matavimo rodiklių aptarimą.

ANTRASIS SKIRSNIS
POKYČIŲ VALDYMO PROCESO MATAVIMO RODIKLIAI

55. Pokyčių valdymo proceso efektyvumui matuoti naudojami rodikliai:

55.1. laiku įvykdytų pokyčių dalis;

55.2. grąžintų vykdyti pokyčių dalis.

56. 55 punkte nurodytų rodiklių siekiamos reikšmės:

Rodiklis	Siekiama reikšmė
Laiku įvykdytų pokyčių dalis	≥ 90 procentai
Grąžintų vykdyti pokyčių dalis	≤ 10 procentai

57. Už pokyčių valdymo proceso efektyvumo matavimo rodiklių kaupimą, analizę ir jų teikimą atsakingas asmuo:

57.1. einamojo mėnesio pradžioje peržiūri praėjusio mėnesio užregistruotus ir vykdytus pokyčius;

57.2. skaičiuoja, ar 55 punkte nurodyti rodikliai atitinka 56 punkte pateiktas siekiamas šių rodiklių reikšmes;

57.3. rengia kiekvieno mėnesio pokyčių rodiklių ataskaitą ir ją pateikia KVTC direktoriui;

57.4. ne rečiau kaip vieną kartą per ketvirtį organizuoja pokyčių valdymo proceso bei jo efektyvumo matavimo rodiklių aptarimą.

TREČIASIS SKIRSNIS
PROBLEMŲ VALDYMO PROCESO MATAVIMO RODIKLIAI

58. Problemų valdymo proceso matavimo rodikliai:

58.1. atvirų problemų kiekis;

58.2. uždarytų problemų kiekis;

58.3. laiku išspręstų problemų kiekis, kur siekiama reikšmė – ne mažiau nei 92 proc. laiku išspręstų problemų.

59. Už matavimo rodiklių kaupimą, analizę ir jų teikimą atsakingas asmuo:

59.1. einamojo mėnesio pradžioje peržiūri praėjusio mėnesio užregistruotas ir uždarytas problemas;

59.2. rengia kiekvieno mėnesio problemų rodiklių ataskaitą ir ją pateikia KVTC direktoriui;

59.3. ne rečiau kaip vieną kartą per ketvirtį organizuoja problemų valdymo proceso bei jo matavimo rodiklių aptarimą.

Papildyta priedu:
Nr. V-338, 2021-05-11, paskelbta TAR 2021-05-11, i. k. 2021-10495

PATVIRTINTA
Lietuvos Respublikos krašto apsaugos ministro
2019 m. liepos 2 d. įsakymu Nr. V-583
(2023 m. gegužės 31 d. įsakymo Nr. V-445
redakcija)

SAUGIOJO TINKLO KIBERNETINIO SAUGUMO POLITIKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Saugiojo tinklo kibernetinio saugumo politika (toliau – Politika) apibrėžia Saugiojo valstybinio duomenų perdavimo tinklo (toliau – Saugusis tinklas) elektroninės informacijos saugos kibernetinėje erdvėje užtikrinimo ir valdymo kryptis, nustato organizacines ir techninės priemones, taikomas užtikrinant Saugiojo tinklo kibernetinę saugą.

2. Saugiojo tinklo kibernetinė sauga įgyvendinama vadovaujantis šia Politika, Saugiojo tinklo valdytojo patvirtintomis Saugiojo tinklo naudotojų administravimo taisyklėmis, Specialiųjų organizacinių ir techninių reikalavimų, taikomų Saugiajam valstybiniam duomenų perdavimo tinklui, juo teikiamoms paslaugoms bei prekių ir paslaugų Saugiajam valstybiniam duomenų perdavimo tinklui teikėjams, aprašu, Saugiojo tinklo veiklos tęstinumo planu, kitais aprašais, procedūromis bei dokumentais, reglamentuojančiais informacijos saugą ir kibernetinį saugumą.

3. Saugiojo tinklo kibernetinės saugos užtikrinimo ir valdymo prioritetinės kryptys:

3.1. tinkamas ir efektyvus informacijos saugumo kibernetinėje erdvėje valdymas siekiant išvengti Saugiojo tinklo veiklos ir juo teikiamų paslaugų sutrikdymo dėl informacijos konfidencialumo, vientisumo bei prieinamumo pažeidimų;

3.2. atitikties teisės aktuose nustatytiems kibernetinio saugumo reikalavimams užtikrinimas;

3.3. gerąją praktiką atitinkančių organizacinių ir techninių kibernetinio saugumo priemonių Saugiajame tinkle įgyvendinimas;

3.4. Saugiojo tinklo veiklos ir juo teikiamų paslaugų tęstinumo užtikrinimas;

3.5. efektyvus kibernetinio saugumo rizikos valdymas ir tinkamų rizikos valdymo priemonių naudojimas, siekiant suvaldyti kibernetinio saugumo rizikas iki priimtino lygio.

4. Politika taikoma Saugiojo tinklo valdytojui, Saugiojo tinklo saugos įgaliotiniui, administratoriams ir kitiems Saugiojo tinklo tvarkytojo darbuotojams, dalyvaujantiems Saugiojo tinklo kibernetinio saugumo užtikrinimo veiklose.

5. Politika parengta vadovaujantis Lietuvos Respublikos kibernetinio saugumo įstatymu, Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ bei atsižvelgiant į tarptautinius informacijos saugos standartus (LST ISO/IEC 27001, LST ISO/IEC 27002 ir kt.).

6. Politikoje vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo 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“, ir kituose saugų duomenų tvarkymą reglamentuojančiuose teisės aktuose.

7. Už Saugiojo tinklo kibernetinio saugumo politikos formavimą, kryptis ir plėtrą atsako Saugiojo tinklo valdytojas.

8. Už Saugiojo tinklo kibernetinio saugumo užtikrinimą ir šios Politikos įgyvendinimą atsako Saugiojo tinklo tvarkytojas.

9. Ši Politika turi būti peržiūrima ne rečiau kaip kartą per metus ir, nustačius poreikį, atnaujinama. Už Politikos priežiūrą atsakingas Saugiojo tinklo saugos įgaliotinis.

II SKYRIUS
AUDITO ŽURNALŲ DUOMENŲ ADMINISTRAVIMAS IR SAUGOJIMAS

10. Siekiant užtikrinti Saugiojo tinklo ir juo teikiamų paslaugų saugumą ir tinkamą veikimą, Saugiajame tinkle yra kaupiami Saugiojo valstybinio duomenų perdavimo tinklo nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro 2018 m. vasario 7 d. įsakymu Nr. V-135 „Dėl Saugiojo valstybinio duomenų perdavimo tinklo nuostatų patvirtinimo“ (toliau – Saugiojo tinklo nuostatai) 14.5 papunktyje nurodyti audito žurnalų duomenys (angl. *log files*) (toliau – Audito žurnalo duomenys), kuriuose fiksuojama Saugiojo tinklo nuostatų 14.6 papunktyje nurodyta informacija.

11. Audito žurnalų duomenys kaupiami ir saugomi centralizuotai techninėje ar programinėje įrangoje ir analizuojami kiekvieną darbo dieną. Apie analizės rezultatus informuojamas Saugiojo tinklo saugos įgaliotinis.

12. Audito žurnalų duomenys saugomi 6 mėnesius nuo įvykio datos užtikrinant visas prasmingas jų turinio reikšmes. Draudžiama ištrinti ir (ar) keisti audito žurnalų duomenis, jie ištrinami tik pasibaigus saugojimo terminui. Audito žurnalų duomenys yra prieinami tik Saugiojo tinklo saugos įgaliotiniui ir kitiems Saugiojo tinklo tvarkytojo paskirtiems atsakingiems asmenims (toliau – atsakingi asmenys) (peržiūros teisėmis).

13. Dėl trikdžių nustojus fiksuoti audito žurnalų duomenis, apie tai nedelsiant, bet ne vėliau kaip per vieną darbo dieną centralizuota techninė ar programinė įranga, skirta audito duomenims saugoti, informuoja Saugiojo tinklo saugos įgaliotinį ir atsakingus asmenis.

14. Įvykus įtartinai veiklai, centralizuota techninė ar programinė įranga, skirta audito duomenims saugoti ir apdoroti, turi užfiksuoti tai audito žurnalų įrašuose ir sukurti pranešimą, kurį matytų atsakingi darbuotojai. Toks pranešimas klasifikuojamas pagal užfiksuotą įvykį.

III SKYRIUS
ĮSIBROVIMŲ APTIKIMAS IR PREVENCIJA

15. Saugiojo tinklo valdymo centre automatizuotomis įsibrovimų aptikimo priemonėmis dvidešimt keturias valandas per parą, septynias dienas per savaitę stebimi įsibrovimai į Saugųjį tinklą analizuojant įeinantį ir išeinantį Saugiojo tinklo duomenų srautą.

16. Įsibrovimų atakų pėdsakai (angl. *attack signature*) atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius.

17. Įsibrovimų atakų pėdsakai Saugiajame tinkle atnaujinami ne vėliau kaip per dvidešimt keturias valandas nuo gamintojo paskelbimo apie naujausius įsibrovimų atakų pėdsakus datos arba ne vėliau kaip per septyniasdešimt dvi valandas nuo gamintojo paskelbimo apie naujausius įsibrovimo atakų pėdsakus datos, jeigu Saugiojo tinklo tvarkytojas atlieka įsibrovimų atakų pėdsakų įdiegimo ir galimo jų poveikio tinklo veiklai vertinimą (testavimą).

18. Saugiojo tinklo tvarkytojas nustato Saugiojo tinklo įsibrovimų aptikimo ir prevencijos procedūras ir joms vykdyti paskiria atsakingus asmenis.

IV SKYRIUS

MOBILIŲJŲ ĮRENGINIŲ NAUDOJIMAS IR KONTROLĖ

19. Saugiojo tinklo veiklai ir paslaugoms teikti naudojami mobilieji įrenginiai – Saugiojo tinklo tvarkytojo nešiojamieji kompiuteriai ir tarnybiniai judriojo ryšio telefonai – naudojami vadovaujantis šiais reikalavimais:

19.1. leidžiama naudoti tik tokius mobiliuosius įrenginius, kurie atitinka šiame skyriuje nurodytus kibernetinio saugumo reikalavimus;

19.2. Saugiojo tinklo tvarkytojo darbuotojai yra atsakingi už jiems priskirtų mobiliųjų įrenginių ir juose esančios informacijos apsaugą;

19.3. prieiga prie nešiojamųjų kompiuterių bei juose esanti informacija turi būti apsaugota slaptažodžiu, o nešiojamuoju kompiuteriu prie Saugiojo tinklo už Saugiojo tinklo tvarkytojo įstaigos ribų galima jungtis tik per virtualų privatų tinklą (angl. *Virtual privat network* (VPN) bei papildomai turi būti naudojamas dviejų faktorių autentifikavimas (2FA). Prieiga prie tarnybinių judriojo ryšio telefonų bei juose esanti informacija turi būti apsaugota naudotojo identifikatoriumi (biometriniais duomenimis ir (arba) PIN kodu);

19.4. Saugiojo tinklo tvarkytojas turi teisę valdyti mobiliuosius įrenginius ir juose įdiegtą programinę įrangą. Mobiliųjų įrenginių techninę ir programinę įrangą diegia ir prižiūri Saugiojo tinklo tvarkytojo sistemų administratorius (-iai). Mobiliuosiuose įrenginiuose turi būti diegiama ir naudojama tik licencijuota ir leistinos programinės įrangos sąraše nurodyta programinė įranga;

19.5. mobiliuosiuose įrenginiuose turi būti reguliariai įdiegiami operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;

19.6. mobiliųjų įrenginių laikmenose duomenys turi būti šifruojami;

19.7. nešiojamuosiuose kompiuteriuose programinėmis priemonėmis turi būti blokuojamos išorinės elektroninės informacijos laikmenos (pvz., USB atmintinės ar pan.), išskyrus atvejus, kai jos yra būtinos administratorių funkcijoms atlikti.

19.8. nešiojamųjų kompiuterių saugiam naudojimui ir kontrolei užtikrinti naudojamas galinių įrenginių aptikimo ir kontrolės sprendimas (angl. *Endpoint detection and control* (EDR), tarnybinių judriojo ryšio telefonų saugiam naudojimui ir kontrolei užtikrinti naudojamas mobiliųjų įrenginių valdymo sprendimas (angl. *Mobile device managemant* (MDM).

V SKYRIUS
GRĖSMIŲ IR PAŽEIDŽIAMUMŲ VALDYMAS

20. Saugiojo tinklo kibernetinio saugumo grėsmių ir pažeidžiamumų valdymą Saugiojo tinklo tvarkytojas atlieka:

20.1. reguliariai skenuodamas Saugiojo tinklo techninę ir programinę įrangą ir vertindamas skenavimo rezultatus (angl. *vulnerability test*);

20.2. ne rečiau, kaip kartą per metus arba įvykus esminiams techniniams Saugiojo tinklo pokyčiams organizuodamas ir atlikdamas Saugiojo tinklo grėsmių ir pažeidžiamumų vertinimą (angl. *penetration test*), kurio tikslas – nustatyti esamus Saugiojo tinklo pažeidžiamumus ir jų rizikos lygį;

20.3. vertindamas iš kitų institucijų gautą informaciją apie galimus Saugiojo tinklo pažeidžiamumus.

21. Grėsmėms ir pažeidžiamumams nustatyti naudojama specializuota programinė įranga (toliau – SPĮ), naudojanti viešai pripažįstamą bendrąją pažeidžiamumų vertinimo metodiką pažeidžiamumo kritiškumui vertinti.

22. Atlikus skenavimą SPĮ automatiškai sugeneruoja ataskaitą, ją įvertinęs Saugiojo tinklo saugos įgaliotinis ir (arba) kitas Saugiojo tinklo tvarkytojo paskirtas (-i) darbuotojas (-ai) parengia vertinimo ataskaitą bei nustatytų grėsmių ir pažeidžiamumų šalinimo planą.

23. Nustatyti pažeidžiamumai vertinami pagal jų poveikį Saugiojo tinklo paslaugų veikimui ir grupuojami bei sprendžiami vadovaujantis šiais kriterijais:

Pažeidžiamumo kritiškumas	Paaiškinimas	Priimtinumas
Labai mažas (*None*)	Tikimybė, kad tinklo ištekliai bus pažeisti, – iki 1 proc.	Priimtinas
Mažas (*Low*)	Tikimybė, kad tinklo ištekliai bus pažeisti, – nuo 2 iki 39 proc.	Priimtinas
Vidutinis (*Medium*)	Tikimybė, tinklo ištekliai bus pažeisti, – nuo 40 iki 69 proc.	Vertinamas
Didelis (*High*)	Tikimybė, kad tinklo ištekliai bus pažeisti, – nuo 70 iki 89 proc.	Nepriimtinas, sprendžiamas nedelsiant
Kritinis (*Critical*)	Tikimybė, kad tinklo ištekliai bus pažeisti, – nuo 90 iki 100 proc.	Nepriimtinas, sprendžiamas nedelsiant

24. Jei pažeidžiamumo išspręsti neįmanoma, priimamos tinkamos riziką valdančios priemonės.

25. Grėsmių ir pažeidžiamumų valdymo procedūras nustato Saugiojo tinklo tvarkytojas.

VI SKYRIUS
KIBERNETINIŲ INCIDENTŲ VALDYMAS

26. Saugiojo tinklo kibernetinių incidentų valdymas organizuojamas ir vykdomas vadovaujantis:

26.1. Nacionalinio kibernetinių incidentų valdymo planu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

26.2. Saugiojo valstybinio duomenų perdavimo tinklo kibernetinių incidentų valdymo planu, patvirtintu Lietuvos Respublikos krašto apsaugos ministro 2021 m. gegužės 31 d. įsakymu Nr. V-379 „Dėl Saugiojo valstybinio duomenų perdavimo tinklo kibernetinių incidentų valdymo plano patvirtinimo“.

27. Kibernetinių incidentų valdymo procese dalyvaujančius asmenis, jų funkcijas ir atsakomybės sritis nustato Saugiojo tinklo tvarkytojas.

VII SKYRIUS
KIBERNETINIO SAUGUMO PRIEMONĖS

28. Saugiojo tinklo kibernetiniam saugumui užtikrinti naudojamos techninės ir programinės kibernetinio saugumo priemonės:

28.1. prieigų kontrolės ir autentifikavimo priemonės (angl. *Network access control*);

28.2. įsibrovimo aptikimo ir prevencijos sistemos (angl. *Intrusion detection/ Intrusion prevention systems*);

28.3. grėsmių ir pažeidžiamumų skenavimo ir nustatymo įrankiai (angl. *Vulnerability scanner*);

28.4. tinklo perimetro saugos priemonės (angl. *Firewall*);

28.5. interneto ir (arba) taikomųjų programų lygmens ugniasienių sistema WAF (angl. *Web application firewalls*);

28.6. interneto ir (arba) taikomųjų programų apsauga nuo DDoS (angl. *Distributed denial-of-service*) atakų;

28.7. didelio efektyvumo kibernetinių atakų prevencijos sistema (DEKAPS);

28.8. kitos kibernetinio saugumo priemonės ir reikalavimai, kaip numatyta Saugiojo tinklo valdytojo patvirtintuose Saugiojo tinklo naudotojų administravimo taisyklėse, Specialiųjų organizacinių ir techninių reikalavimų, taikomų Saugiajam valstybiniam duomenų perdavimo tinklui, juo teikiamoms paslaugoms bei prekių ir paslaugų Saugiajam valstybiniam duomenų perdavimo tinklui teikėjams, apraše ir Saugiojo tinklo veiklos tęstinumo plane.

29. Kibernetinio saugumo priemonės diegiamos bei jų parametrai keičiami Saugiojo tinklo valdytojo patvirtintų Saugiojo tinklo incidentų, pokyčių ir problemų valdymo tvarkos aprašo nustatyta tvarka.

VIII SKYRIUS
MOKYMAI

30. Saugiojo tinklo saugos įgaliotinis ne rečiau kaip kartą per metus inicijuoja Saugiojo tinklo tvarkytojo darbuotojų mokymą informacijos saugos, kibernetinio saugumo klausimais, įvairiais būdais (žodžiu, elektroniniu paštu, dokumentų valdymo sistemoje ar kt.) konsultuoja darbuotojus ir teikia jiems susijusią aktualią informaciją.

31. Saugiojo tinklo saugos įgaliotinis, administratoriai ir kiti tvarkytojo darbuotojai, dalyvaujantys Saugiojo tinklo kibernetinio saugumo veikloje, dalyvauja Lietuvos Respublikos krašto apsaugos ministerijos, Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos ir kitų institucijų organizuojamose kibernetinio saugumo pratybose.

32. Saugiojo tinklo tvarkytojas telefonu, elektroniniu paštu ir kitais būdais teikia informaciją Saugiojo tinklo naudotojams kibernetinio saugumo Saugiajame tinkle klausimais, informuoja juos apie galimas kibernetines grėsmes ir rizikas.

33. Saugiojo tinklo naudotojai ne rečiau kaip kartą per metus organizuoja informacijos saugos mokymus savo darbuotojams.

_____

Priedų pakeitimai:

Prisijungimo+prie+ST+apraso+1+priedas_2022-03-18 (pagal V-94)
Priedo pakeitimai:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436
Nr. V-94, 2023-02-03, paskelbta TAR 2023-02-03, i. k. 2023-02047

Prisijungimo+prie+ST+apraso+2+priedas_2022-03-18 (pagal V-94)
Priedo pakeitimai:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436
Nr. V-94, 2023-02-03, paskelbta TAR 2023-02-03, i. k. 2023-02047

Prisijungimo+prie+ST+apraso+3+priedas_2022-03-18 (pagal V-548)
Priedo pakeitimai:
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436
Nr. V-94, 2023-02-03, paskelbta TAR 2023-02-03, i. k. 2023-02047

Nr. V-548, 2023-07-03, paskelbta TAR 2023-07-03, i. k. 2023-13642

Prisijungimo+prie+ST+apraso+4+priedas_2022-03-18 (pagal V-473)
Priedo pakeitimai:
Nr. V-473, 2022-06-22, paskelbta TAR 2022-06-22, i. k. 2022-13389

Pakeitimai:

1.
Lietuvos Respublikos krašto apsaugos ministerija, Įsakymas
Nr. V-393, 2020-05-19, paskelbta TAR 2020-05-20, i. k. 2020-10651
Dėl krašto apsaugos ministro 2019 m. liepos 2 d. įsakymo Nr. V-583 „Dėl Saugiojo valstybinio duomenų perdavimo tinklo veiklą užtikrinančių dokumentų patvirtinimo“ pakeitimo

2.
Lietuvos Respublikos krašto apsaugos ministerija, Įsakymas
Nr. V-286, 2021-04-22, paskelbta TAR 2021-04-22, i. k. 2021-08376
Dėl Lietuvos Respublikos krašto apsaugos ministro 2019 m. liepos 2 d. įsakymo Nr. V-583 „Dėl Saugiojo valstybinio duomenų perdavimo tinklo veiklą užtikrinančių dokumentų patvirtinimo“ pakeitimo

3.
Lietuvos Respublikos krašto apsaugos ministerija, Įsakymas
Nr. V-338, 2021-05-11, paskelbta TAR 2021-05-11, i. k. 2021-10495
Dėl Lietuvos Respublikos krašto apsaugos ministro 2019 m. liepos 2 d. įsakymo Nr. V-583 „Dėl Saugiojo valstybinio duomenų perdavimo tinklo veiklą užtikrinančių dokumentų patvirtinimo“ pakeitimo

4.
Lietuvos Respublikos krašto apsaugos ministerija, Įsakymas
Nr. V-596, 2021-08-25, paskelbta TAR 2021-08-25, i. k. 2021-17891
Dėl krašto apsaugos ministro 2019 m. liepos 2 d. įsakymo Nr. V-583 „Dėl Saugiojo valstybinio duomenų perdavimo tinklo veiklą užtikrinančių dokumentų patvirtinimo“ pakeitimo

5.
Lietuvos Respublikos krašto apsaugos ministerija, Įsakymas
Nr. V-831, 2021-10-26, paskelbta TAR 2021-10-26, i. k. 2021-22243
Dėl Lietuvos Respublikos krašto apsaugos ministro 2019 m. liepos 2 d. įsakymo Nr. V-583 „Dėl Saugiojo valstybinio duomenų perdavimo tinklo veiklą užtikrinančių dokumentų patvirtinimo“ pakeitimo

6.
Lietuvos Respublikos krašto apsaugos ministerija, Įsakymas
Nr. V-268, 2022-03-28, paskelbta TAR 2022-03-28, i. k. 2022-06064
Dėl Lietuvos Respublikos krašto apsaugos ministro 2019 m. liepos 2 d. įsakymo Nr. V-583 „Dėl Saugiojo valstybinio duomenų perdavimo tinklo veiklą užtikrinančių dokumentų patvirtinimo“ pakeitimo

7.
Lietuvos Respublikos krašto apsaugos ministerija, Įsakymas
Nr. V-473, 2022-06-22, paskelbta TAR 2022-06-22, i. k. 2022-13389
Dėl Lietuvos Respublikos krašto apsaugos ministro 2019 m. liepos 2 d. įsakymo Nr. V-583 „Dėl Saugiojo valstybinio duomenų perdavimo tinklo veiklą užtikrinančių dokumentų patvirtinimo“ pakeitimo

8.
Lietuvos Respublikos krašto apsaugos ministerija, Įsakymas
Nr. V-770, 2022-09-23, paskelbta TAR 2022-09-23, i. k. 2022-19436
Dėl Lietuvos Respublikos krašto apsaugos ministro 2019 m. liepos 2 d. įsakymo Nr. V-583 „Dėl Saugiojo valstybinio duomenų perdavimo tinklo veiklą užtikrinančių dokumentų patvirtinimo“ pakeitimo

9.
Lietuvos Respublikos krašto apsaugos ministerija, Įsakymas

Nr. V-207, 2021-03-25, paskelbta TAR 2022-12-05, i. k. 2022-24736
Dėl Lietuvos Respublikos krašto apsaugos ministro 2019 m. liepos 2 d. įsakymo Nr. V-583 „Dėl Saugiojo tinklo veiklą užtikrinančių dokumentų patvirtinimo“ pakeitimo

10.
Lietuvos Respublikos krašto apsaugos ministerija, Įsakymas
Nr. V-94, 2023-02-03, paskelbta TAR 2023-02-03, i. k. 2023-02047
Dėl Lietuvos Respublikos krašto apsaugos ministro 2019 m. liepos 2 d. įsakymo Nr. V-583 „Dėl Saugiojo valstybinio duomenų perdavimo tinklo veiklą užtikrinančių dokumentų patvirtinimo“ pakeitimo

11.
Lietuvos Respublikos krašto apsaugos ministerija, Įsakymas
Nr. V-445, 2023-05-31, paskelbta TAR 2023-05-31, i. k. 2023-10655
Dėl Lietuvos Respublikos krašto apsaugos ministro 2019 m. liepos 2 d. įsakymo Nr. V-583 „Dėl Saugiojo valstybinio duomenų perdavimo tinklo veiklą užtikrinančių dokumentų patvirtinimo“ pakeitimo

12.
Lietuvos Respublikos krašto apsaugos ministerija, Įsakymas
Nr. V-548, 2023-07-03, paskelbta TAR 2023-07-03, i. k. 2023-13642
Dėl Lietuvos Respublikos krašto apsaugos ministro 2019 m. liepos 2 d. įsakymo Nr. V-583 „Dėl Saugiojo valstybinio duomenų perdavimo tinklo veiklą užtikrinančių dokumentų patvirtinimo“ pakeitimo