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 dalimi ir 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:

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.

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 2020 m. sausio 1 d. turi įvykdyti šio nutarimo 1 punktu patvirtintų teisės aktų reikalavimus.

Vidaus reikalų ministras,
pavaduojantis krašto apsaugos ministrą Eimutis Misiūnas

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

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 ir papildomų 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 sąrašą (toliau – naudotojas), 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. Paslaugų kiekybiniai ir kokybiniai rodikliai, Saugiuoju tinklu teikiamos standartinės elektroninių ryšių paslaugos (toliau – standartinės paslaugos) ir Saugiuoju tinklu teikiamos papildomos elektroninių ryšių paslaugos (toliau – papildomos paslaugos) nurodomos Tvarkos aprašo 1 priede.

II SKYRIUS
PRISIJUNGIMO PRIE SAUGIOJO TINKLO IR ATSIJUNGIMO NUO JO SĄLYGOS

PIRMASIS SKIRSNIS
PRISIJUNGIMAS PRIE SAUGIOJO TINKLO

5. Naudotojas, jungdamasis prie Saugiojo tinklo, privalo:

5.1. paslaugų teikimo vietoje ar vietose įrengti Saugiojo tinklo įrangai skirtą patalpą, kurioje:

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

5.1.1.1. oro temperatūra 10–30 ^{o}C;

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

5.1.2. elektros maitinimas ir elektros apsaugos priemonės turi atitikti Saugiojo tinklo įrangos gamintojo nustatytus ir naudotojo keliamus papildomus reikalavimus, avarinio ir rezervinio maitinimo reikalavimus.

5.1.3. Pagrindiniai elektros maitinimo reikalavimai:

5.1.3.1. įtampa 230 V, 50 Hz;

5.1.3.2. galingumas 0,7 kW;

5.1.3.3. įžeminimas pagal standartą LST ETS 300 253;

5.1.4. įrengta gaisro pavojaus sistema, atitinkanti LST EN 54 grupės standartų reikalavimus;

5.1.5. reagavimas į gaisro pavojaus signalą užtikrinamas visą parą darbo, poilsio ir švenčių dienomis;

5.1.6. patekimas į Saugiojo tinklo įrangai skirtą patalpą kontroliuojamas mechaniniais užraktais arba elektronine įeigos kontrolės sistema;

5.2. užtikrinti elektros maitinimą iš 230 V, 50 Hz maitinimo tinklo, kurio galia turi užtikrinti Saugiojo tinklo įrangos elektros maitinimo reikmes. Rezervinis ir avarinis maitinimas numatomas pagal naudotojo nuosavo tinklo veikimo reikalavimus;

5.3. užtikrinti galimybę Saugiojo tinklo tvarkytojui įrengti vietinę prieigos dalį (optinių ar varinių gijų kabeliu) Saugiojo tinklo įrangai skirtose patalpose nuo (iki) Saugiojo tinklo įrangos įrengimo vietos;

5.4. 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“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas), bei šiuose dokumentuose keliamų reikalavimų įgyvendinimu;

5.5. užtikrinti eterneto *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;

5.6. užtikrinti, kad jo informacinių išteklių tarnybinės stotys, vartotojų darbo vietų kompiuteriai ir kita įranga, kuri siųs ir gaus duomenis per Saugųjį tinklą, turėtų fiksuotus vidinius IP adresus naudotojo tinkle. Vidiniai naudotojo kompiuterių tinklo adresai negali būti iš IP adresų srities 10.200.X.X–10.255.X.X;

5.7. patvirtinti vidinius teisės aktus, kuriuose:

5.7.1. numatoma asmenų patekimo į Saugiojo tinklo įrangai skirtą patalpą kontrolė ir apribojimai;

5.7.2. numatomas baigtinis asmenų, turinčių teisę patekti į Saugiojo tinklo įrangai skirtą patalpą, sąrašas;

5.8. užtikrinti galimybę Saugiojo tinklo tvarkytojo atstovams patekti į Saugiojo tinklo įrangai skirtas patalpas tokia tvarka:

5.8.1. naudotojas išduos Saugiojo tinklo tvarkytojo atstovams nuolatinį leidimą patekti į Saugiojo tinklo įrangai skirtas patalpas visą parą arba užtikrins, kad Saugiojo tinklo tvarkytojo atstovams bus paskirtas lydintis asmuo, kuris užtikrins patekimą į Saugiojo tinklo įrangai skirtas patalpas visą parą, ne vėliau kaip per 1 (vieną) valandą nuo Saugiojo tinklo tvarkytojo pranešimo gavimo momento, kai Saugiojo tinklo tvarkytojo atstovams būtina patekti į Saugiojo tinklo įrangai skirtas patalpas;

5.8.2. naudotojas užtikrins, kad Saugiojo tinklo tvarkytojo atstovai, atliekantys Saugiojo tinklo įrangos įrengimo, priežiūros ar remonto darbus Saugiojo tinklo įrangai skirtose patalpose, galės naudotojo nustatyta tvarka įsinešti ir išsinešti įrankius, medžiagas, Saugiojo tinklo įrangą ir jos dalis, matavimo įrangą, reikalingą Saugiojo tinklo įrangos įrengimui, priežiūrai ar remontui atlikti;

5.8.3. naudotojas užtikrins Saugiojo tinklo tvarkytojo atstovams, atliekantiems Saugiojo tinklo įrangos įrengimo, priežiūros ar remonto darbus Saugiojo tinklo įrangai skirtose patalpose, tinkamas darbo sąlygas;

5.9. 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 (penkias) darbo dienas nuo įvykusių pasikeitimų dienos pateikti Saugiojo tinklo tvarkytojui.

6. Naudotojas per 30 (trisdešimt) darbo dienų nuo Saugiojo tinklo naudotojų sąrašo patvirtinimo Saugiojo tinklo tvarkytojui turi pateikti:

6.1. Saugiojo tinklo įrangos įrengimo vietų su prisijungimo prie Saugiojo tinklo adresais sąrašą;

6.2. informaciją apie Tvarkos aprašo 5 punkte nustatytų reikalavimų įgyvendinimą.

7. Saugiojo tinklo tvarkytojas ne vėliau kaip per 20 (dvidešimt) darbo dienų nuo Tvarkos aprašo 6 punkte nurodytos informacijos gavimo:

7.1. teikia užklausą Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos (toliau – NKSC) apie naudotojo pateiktų kibernetinio saugumo politikos ir jos

įgyvendinimo dokumentų projektų dėl atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams, pateiktiems Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, suderinimo būklę;

7.2. parengia šalintinų trūkumų, jei jų buvo nustatyta, sąrašą, nustato jų pašalinimo terminą ir pateikia sąrašą naudotojui;

7.3. jei nenustatyta trūkumų – parengia prisijungimo prie Saugiojo tinklo plano projektą ir teikia jį tvirtinti Lietuvos Respublikos krašto apsaugos ministerijai.

8. Naudotojas, pašalinęs trūkumus, nurodytus Tvarkos aprašo 7.2 papunktyje nurodytame šalintinų trūkumų sąraše, informuoja Saugiojo tinklo tvarkytoją pakartotinai teikdamas Tvarkos aprašo 6 punkte nurodytą informaciją. Saugiojo tinklo tvarkytojas, atsižvelgdamas į naudotojo pakartotinai pateiktą informaciją, parengia ir teikia Krašto apsaugos ministerijai prisijungimo prie Saugiojo tinklo plano projektą arba pakartotinai teikia naudotojui Tvarkos aprašo 7.2 papunktyje nurodytą informaciją.

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

10. Prisijungimo prie Saugiojo tinklo akte nurodoma:

10.1. Saugiojo tinklo tvarkytojas ir naudotojas;

10.2. naudotojui perduodama Saugiojo tinklo įranga;

10.3. prisijungimo prie Saugiojo tinklo adresas ar adresai;

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

10.5. naudotojo prisijungimo prie Saugiojo tinklo data;

10.6. naudotojo tinklo ar jo dalies, prijungtos prie Saugiojo tinklo, ribos;

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

11. Pasikeitus prisijungimo prie Saugiojo tinklo adresui ar naudotojui prireikus prisijungti prie Saugiojo tinklo nauju adresu, naudotojas turi pateikti Saugiojo tinklo tvarkytojui Tvarkos aprašo 6.2 papunktyje nurodytą informaciją, kiek ji yra susijusi su naujame prisijungimo prie Saugiojo tinklo adrese nurodyta Saugiojo tinklo prieigos vieta.

12. Saugiojo tinklo tvarkytojas, gavęs 11 punkte nurodytą informaciją, naudotojui naują Saugiojo tinklo prieigos vietą suteikia *mutatis mutandis* taikydamas Tvarkos aprašo 7–10 punktus.

ANTRASIS SKIRSNIS
ATSIJUNGIMAS NUO SAUGIOJO TINKLO

13. Naudotojas, išbrauktas iš Saugiojo tinklo naudotojų sąrašo, netenka teisės naudotis Saugiuoju tinklu ir Saugiojo tinklo tvarkytojas per 20 (dvidešimt) darbo dienų Krašto apsaugos ministerijai pateikia atjungimo nuo Saugiojo tinklo plano projektą.

14. Naudotojas, išbrauktas iš Saugiojo tinklo naudotojų sąrašo, Saugiojo tinklo tvarkytojui per 30 (trisdešimt) kalendorinių dienų nuo atsijungimo nuo Saugiojo tinklo dienos turi grąžinti pagal prisijungimo prie Saugiojo tinklo aktą perduotą Saugiojo tinklo įrangą.

III SKYRIUS
PASLAUGŲ TEIKIMO SAUGIUOJU TINKLU SĄLYGOS

PIRMASIS SKIRSNIS
PASLAUGŲ UŽSAKYMAS

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

16. Standartinės paslaugos, nurodytos Tvarkos aprašo 1 priedo 1–3 punktuose, teikiamos visiems naudotojams, prisijungusiems prie Saugiojo tinklo, netaikant papildomų sąlygų.

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

18. Naudotojas, siekdamas gauti standartinę paslaugą, nurodytą Tvarkos aprašo 1 priedo 4 punkte, užpildo Paraiškos dėl sąveikos su Europos Sąjungos ir jos valstybių narių institucijų valdomais informaciniais ištekliais paslaugos užsakymo formą (Tvarkos aprašo 2 priedas) ir ją pateikia Saugiojo tinklo tvarkytojui.

19. Naudotojas, siekdamas gauti standartinę paslaugą, nurodytą Tvarkos aprašo 1 priedo 5 punkte, užpildo Paraiškos dėl valstybės valdomų elektroninių ryšių tinklų, kurie naudojami vykdant valstybines mobilizacines užduotis, dalių sujungimo paslaugos užsakymo formą (Tvarkos aprašo 3 priedas) ir pateikia ją Saugiojo tinklo tvarkytojui.

20. Naudotojas, siekdamas gauti papildomą paslaugą ar paslaugas, užpildo Paraiškos dėl papildomų duomenų perdavimo paslaugos, sąveikos su Europos Sąjungos ir jos valstybių narių institucijų valdomais informaciniais ištekliais paslaugos ir valstybės valdomų elektroninių ryšių tinklų, kurie naudojami vykdant valstybines mobilizacines užduotis, dalių sujungimo paslaugos užsakymo formą (Tvarkos aprašo 4 priedas) ir ją pateikia Saugiojo tinklo tvarkytojui.

21. Saugiojo tinklo tvarkytojas, gavęs bet kurią iš Tvarkos aprašo 18–20 punktuose nurodytų paraiškų:

21.1. ne vėliau kaip per 10 (dešimt) darbo dienų nuo paraiškos gavimo naudotojui pateikia šalintinų trūkumų sąrašą arba

21.2. ne vėliau kaip per 10 (dešimt) darbo dienų nuo paraiškos gavimo pateikia naudotojui Saugiojo tinklo paslaugų teikimo akto projektą ir ne vėliau kaip per Tvarkos aprašo 22 punkte nurodytą terminą naudotojui pradeda teikti paraiškoje nurodytą paslaugą (paslaugas) arba, jeigu su paslaugos gavėju suderinamas ankstesnis terminas, teikdamas papildomų paslaugų teikimo akto projektą patvirtina, kad paslaugos teikimas bus pradėtas suderintu terminu.

22. Paslaugų teikimo pradžios terminai:

22.1. 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 patvirtinimo;

22.2. standartinė paslauga, nurodyta Tvarkos aprašo 1 priedo 4 punkte, pradedama teikti ne vėliau kaip per 6 mėn. nuo paraiškos gavimo datos;

22.3. standartinė paslauga, nurodyta Tvarkos aprašo 1 priedo 5 punkte, pradedama teikti ne vėliau kaip per 9 mėnesius nuo paraiškos gavimo datos;

22.4. papildomos paslaugos pradedamos teikti ne vėliau kaip per 9 mėnesius nuo paraiškos gavimo datos.

23. Papildomų paslaugų gavimo faktas patvirtinamas, kai Saugiojo tinklo tvarkytojas ir naudotojas pasirašo papildomų paslaugų teikimo aktą.

24. Papildomų paslaugų teikimo akte nurodoma:

24.1. Saugiojo tinklo tvarkytojas ir naudotojas;

24.2. naudotojui perduodama Saugiojo tinklo įranga;

24.3. papildomų paslaugų teikimo adresas ar adresai;

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

24.5. teikiamos papildomos paslaugos, jų kokybiniai ir kiekybiniai rodikliai;

24.6. papildomų paslaugų teikimo pradžios data;

24.7. Saugiojo tinklo valdytojo patvirtinta papildomų paslaugų teikimo kaina;

24.8. Saugiojo tinklo tvarkytojo sąskaita;

24.9. kitos Tvarkos aprašo 45 punkte nurodytos sąlygos, dėl kurių susitaria Saugiojo tinklo tvarkytojas ir naudotojas.

25. Papildomų paslaugų teikimo aktas įsigalioja nuo jos pasirašymo dienos ir galioja iki naudotojo išbraukimo iš Saugiojo tinklo naudotojų sąrašo arba iki papildomų paslaugų teikimo akte numatyto termino.

ANTRASIS SKIRSNIS
PASLAUGŲ KEITIMAS IR TEIKIMO NUTRAUKIMAS

26. Naudotojas turi teisę bet kada teikti naują Tvarkos aprašo 18–20 punktuose nurodytą paraišką. Paslaugos teikiamos pagal vėliausiai pateiktą paraišką.

27. 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 (penkias) darbo dienas nuo šiame punkte nurodytos funkcijos panaikinimo dienos turi užpildyti atitinkamą Tvarkos aprašo 2–4 prieduose nurodytų paraiškų formą dėl turimos paslaugos teikimo nutraukimo ir informuoti Saugiojo tinklo tvarkytoją apie šiame punkte nurodytos funkcijos panaikinimą.

28. Saugiojo tinklo tvarkytojas, gavęs Tvarkos aprašo 27 punkte nurodytą informaciją, ne vėliau kaip 10 (dešimt) darbo dienų nutraukia atitinkamos standartinės paslaugos, numatytos Tvarkos aprašo 1 priedo 4 ar 5 punkte, teikimą naudotojui.

29. Teikiamos papildomos paslaugos kiekybiniai ir kokybiniai rodikliai, papildomos paslaugos teikimo terminas keičiamas naudotojui pateikus Tvarkos aprašo 20 punkto nustatyta tvarka naują paraišką.

30. Saugiojo tinklo tvarkytojas turi teisę atsisakyti keisti papildomos paslaugos kiekybinius ir kokybinius rodiklius, papildomos paslaugos teikimo terminą dėl galimų neproporcingų išlaidų,

atsirandančių Saugiojo tinklo tvarkytojui dėl nurodyto keitimo. Šiame punkte nurodytas atsisakymas turi būti pagrįstas.

IV SKYRIUS
PASLAUGŲ TEIKIMO SAUGIUOJU TINKLU TAISYKLĖS

PIRMASIS SKIRSNIS
TEISĖS, PAREIGOS IR ATSAKOMYBĖ

31. Saugiojo tinklo tvarkytojo teisės:

31.1. be išankstinio perspėjimo, įvykus saugumo incidentui arba esant akivaizdžiai saugumo incidento grėsmei, sustabdyti paslaugos teikimą 48 val., apie paslaugos teikimo sustabdymą informuojant naudotoją per 1 (vieną) darbo dieną;

31.2. pasitelkti trečiuosius asmenis įsipareigojimams vykdyti.

32. Naudotojo pareigos:

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

32.2. užtikrinti, kad naudotojo patalpose esančios Saugiojo tinklo tvarkytojo elektroninių ryšių linijos, Saugiojo tinklo įranga nebūtų sugadintos, pažeistos, sunaikintos dėl naudotojo ar trečiųjų asmenų kaltės;

32.3. užtikrinti paslaugoms teikti reikalingos elektros energijos tiekimą ir tvarkingą elektros instaliaciją;

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

32.5. ne vėliau kaip per 1 (vieną) darbo dieną informuoti Saugiojo tinklo tvarkytoją apie paslaugos teikimo sutrikimus;

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

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

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

32.9. užtikrinti, kad naudotojo tinklų tarnybinės stotys, darbo vietos ir kita įranga, siunčianti ir gaunanti elektroninę informaciją per Saugųjį tinklą, turėtų fiksuotus vidinius IP adresus naudotojo tinkle.

33. Saugiojo tinklo tvarkytojo pareigos:

33.1. paskirti įgaliotą asmenį ar asmenis, kurie atstovaus Saugiojo tinklo tvarkytojui prisijungimo prie Saugiojo tinklo techninio administravimo klausimais, naudotojams 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 (penkias) darbo dienas nuo įvykusių pasikeitimų dienos pateikti naudotojams;

33.2. teikti, įrengti, prižiūrėti, keisti bei išmontuoti Saugiojo tinklo įrangą ir šalinti jos gedimus;

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

33.4. imtis priemonių, kurios užtikrintų Saugiojo tinklo ir paslaugų saugumą, vientisumą, patikimumą, paslaugų suderinamumą;

33.5. šalinti paslaugų teikimo sutrikimus, jeigu paslaugos teikimo kiekybiniai ir kokybiniai rodikliai yra kitokie, nei nurodyta Tvarkos aprašo 1 priede.

34. Naudotojui draudžiama savavališkai taisyti Saugiojo tinklo įrangą ir (ar) ją modifikuoti.

35. Saugiojo tinklo tvarkytojas neatsako už:

35.1. naudotojo tinklo bei kitų įrenginių sutrikimus, gedimus, atsiradusius ne dėl Saugiojo tinklo tvarkytojo kaltės, ir už tokių gedimų, sutrikimų šalinimą;

35.2. Saugiuoju tinklu perduodamos informacijos turinį;

35.3. kenkimo programinės įrangos ar kitų duomenų, pažeidžiančių teisės aktus ar sukeliančių žalą, siuntimą per Saugųjį tinklą bei Saugiojo tinklo naudojimą Lietuvos Respublikos įstatymais draudžiamai veiklai;

35.4. paslaugos teikimo nutraukimą ir (ar) taip naudotojui padarytą žalą, jeigu tai įvyko dėl naudotojo ar trečiųjų asmenų kaltės.

ANTRASIS SKIRSNIS
PASLAUGŲ TEIKIMO SUSTABDYMO SĄLYGOS

36. Paslaugų teikimas naudotojui stabdomas, jei naudotojas:

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

36.2. atliko veiksmus, kurie galėjo pažeisti arba sukelti grėsmę pažeisti Saugųjį tinklą 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;

36.3. siuntė informaciją ar vykdė veiklą, nurodytą Tvarkos aprašo 35.3 papunktyje;

36.4. laiku neatsiskaito su Saugiojo tinklo tvarkytoju už suteiktas papildomas paslaugas.

37. Tvarkos aprašo 36.4 papunktyje nurodytu atveju stabdomas tik papildomų paslaugų teikimas.

38. Sprendimą dėl paslaugų teikimo stabdymo priima Saugiojo tinklo tvarkytojas ir raštu įspėja naudotoją ne vėliau kaip prieš 7 (septynias) darbo dienas iki paslaugų teikimo sustabdymo dienos.

39. Saugiojo tinklo tvarkytojui sustabdžius paslaugų teikimą naudotojui, paslaugų teikimas neatnaujinamas tol, kol nepanaikinamos tokio sustabdymo priežastys. Saugiojo tinklo tvarkytojas paslaugų teikimą atnaujina ne vėliau kaip kitą dieną, kai naudotojas pašalina paslaugų teikimo sustabdymo priežastis ir apie tai informuoja Saugiojo tinklo tvarkytoją. Tvarkos aprašo 36.1–36.2 papunkčiuose nurodytais atvejais paslaugų teikimas turi būti atnaujintas naudotojui pateikus informaciją iš NKSC apie grėsmių Saugiajam tinklui sukelto incidento išsprendimą.

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

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

TREČIASIS SKIRSNIS
MOKĖJIMAS UŽ PAPILDOMŲ PASLAUGŲ TEIKIMĄ

42. Visos numatytos sumos apskaičiuojamos ir mokėjimai atliekami eurais.

43. Naudotojas atsiskaito su Saugiojo tinklo tvarkytoju už tinkamai atliktą papildomą paslaugą kas mėnesį, ne vėliau kaip per 30 (trisdešimt) kalendorinių dienų nuo dienos, kai pradedama teikti papildoma paslauga ir naudotojas patvirtina PVM sąskaitą faktūrą.

44. Tvarkos aprašo 41 punkte minimas mokėjimas įvykdomas atitinkamą sumą pervedus į papildomų paslaugų teikimo akte nurodytą Saugiojo tinklo tvarkytojo sąskaitą.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

45. Saugiojo tinklo tvarkytojas ir naudotojas turi teisę raštu susitarti dėl papildomų paslaugų teikimo sąlygų ir taisyklių, neprieštaraujančių Tvarkos aprašo nuostatoms, keisti Tvarkos apraše numatytus terminus.

_____

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 teikėjai ir gavėjai, jų funkcijos, teisės ir pareigos;

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“, kuriame reglamentuojama duomenų sauga: 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;

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.

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 šiuos minimalius apsaugos reikalavimus:

11.10.1. technologinės spintos, jų užraktai, tvirtinimo būdas:

11.10.1.1. technologinės spintos sienelės turi būti ne plonesnės kaip 1,2 mm;

11.10.1.2. technologinėse spintose, kurių korpuso konstrukcija yra ardoma, turi būti įdiegti atidarymo kontrolės įtaisai ir jutikliai, apsaugantys nuo fizinių išorinių veiksnių;

11.10.1.3. technologinių spintų ventiliacijos grotelių ertmės turi būti ne didesnės kaip 7 mm ir su papildoma apsauga nuo tiesioginio fizinio kontakto su įranga;

11.10.1.4. spyna technologinės spintos viduje turi būti įtvirtinta taip, kad būtų apsaugota nuo mechaninio poveikio iš išorės (išorinėje spintos durelių pusėje turi būti tik spynos anga raktui arba kodinio užrakto valdymo įrenginiai);

11.10.2. patalpos:

11.10.2.1. sienos ir perdangos, kurių storis neatitinka Įslaptintos informacijos fizinės apsaugos reikalavimų ir jų įgyvendinimo tvarkos aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 820 „Dėl Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo įgyvendinimo“, 2 priedo 2.1.2–2.1.9 papunkčiuose nustatytų

reikalavimų, turi būti sumūrytos iš plytų, blokelių arba sukonstruotos iš metalo lakštų, masyvinės medienos ar panašių, analogišką atsparumą įsilaužimui užtikrinančių medžiagų;

11.10.2.2. durų varčia ir stakta turi būti iš ne mažesnio kaip 1,2 mm storio metalo lakštų, masyvinės medienos, drožlių plokščių, faneros, stiklo ar panašių, analogišką atsparumą įsilaužimui užtikrinančių medžiagų, duryse turi būti įrengtas vienas užraktas su cilindrine šerdimi arba plokštelinis užraktas;

11.10.2.3. langų rėmai turi būti pagaminti iš ne mažesnio kaip 60 mm storio masyvinės medienos ar panašių, analogišką atsparumą įsilaužimui užtikrinančių medžiagų, stiklas turi būti padengtas apsaugine plėvele;

11.10.2.4. grotos turi būti iš ne plonesnių kaip 10 mm skersmens plieninių strypų arba analogišką atsparumą įsilaužimui užtikrinančių medžiagų ir įtvirtintos taip, kad jų nebūtų galima išmontuoti atsukant varžtus ar kitaip nuimant tvirtinimus. Angos tarp strypų turi būti ne didesnės kaip 225 cm^2. Varstomosios grotos turi būti rakinamos ne mažiau kaip dviejose vietose užraktais, kurių cilindrinių šerdžių testavimas atliktas pagal Lietuvos standartą LST EN 1303, ir atitikti ne žemesnės kaip 4 saugumo klasės reikalavimus; kabamųjų spynų testavimas atliktas pagal Lietuvos standartą LST EN 12320 ir atitikti ne žemesnio kaip 4 lygio reikalavimus;

11.10.2.5. apsauginių žaliuzių profiliai turi būti pagaminti iš ne plonesnės kaip 0,42 mm storio skardos.

11.11. Teritorijos tvoros, vartai, užtvarai ir turniketai turi būti įrengti sudarant kliūtis, reikalaujančias fizinių pastangų joms įveikti (pralįsti, perlipti, peršokti ar sugadinti).

11.12. Transporto priemonių įvažiavimas į teritoriją ir judėjimas joje turi būti kontroliuojamas.

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. Vykdant Saugiojo tinklo saugos rizikos analizę turi būti atliekamas ir Saugiojo tinklo pažeidžiamumo įvertinimas (angl. *penetration test*).

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.

_____