PATVIRTINTA
Valstybinės kainų ir energetikos
kontrolės komisijos pirmininko
2017 m. d. įsakymu Nr. O1-

VALSTYBINĖS KAINŲ IR ENERGETIKOS KONTROLĖS KOMISIJOS DUOMENŲ SURINKIMO IR ANALIZĖS INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės kainų ir energetikos kontrolės komisijos (toliau – Komisija) duomenų surinkimo ir analizės informacinės sistemos (toliau – DSAIS) saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) nustato tvarką, pagal kurią turi būti saugiai tvarkoma DSAIS elektroninė informacija.

2. Taisyklės parengtos vadovaujantis:

2.1. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Saugos dokumentų turinio gairių aprašu, Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašu, patvirtintu 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“;

2.2. Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;

2.3. Valstybinės kainų ir energetikos kontrolės komisijos duomenų surinkimo ir analizės informacinės sistemos duomenų saugos nuostatais, patvirtintais Komisijos pirmininko 2013 m. gegužės 7 d. įsakymu Nr.O1-40 „Dėl Valstybinės kainų ir energetikos kontrolės komisijos duomenų surinkimo ir analizės informacinės sistemos įsteigimo ir jos nuostatų patvirtinimo bei duomenų surinkimo ir analizės informacinės sistemos duomenų saugos nuostatų patvirtinimo“;

2.4. Lietuvos standartais LST ISO/IEC 27001:2013, LST ISO/IEC 27002:2014, taip pat kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais, apibūdinančiais informacijos saugos valdymą ir saugų duomenų tvarkymą.

3. Taisyklėse vartojamos sąvokos:

3.1. **Saugos įgaliotinis** – Komisijos paskirtas valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį, koordinuojantis ir prižiūrintis saugos politikos įgyvendinimą DSAIS;

3.2. **DSAIS administratorius** – Komisijos paskirtas valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį, vykdantis DSAIS operacinės sistemos, taikomosios programinės įrangos, naudotojų teisių, duomenų tvarkymo priežiūrą;

3.3. **Ūkio subjektas** – reguliuojamą energetikos veiklą vykdantis ūkio subjektas, turintis pareigą teikti Komisijai duomenis ir kitą informaciją per DSAIS;

3.4. **DSAIS ataskaitų administratorius** – Komisijos paskirtas valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį, administruoti tik savo sektoriui priskirtus ataskaitų šablonus, formų šablonus, prižiūrėti ataskaitų pateikimo terminus, tvarkyti ataskaitų darbo sekas;

3.5. **DSAIS vidinis naudotojas** – Komisijos paskirtas valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį, ataskaitų darbo sekose priskirtas atsakingo naudotojo arba vykdytojo rolei;

3.6. **DSAIS išorinis naudotojas** – Ūkio subjektas (Ūkio subjekto atstovas), kuris naudojasi DSAIS ataskaitoms teikti ir kitiems susijusiems veiksmams atlikti;

3.7. **DSAIS naudotojas** – DSAIS vidinis ir išorinis naudotojai;

3.8. **Virtualus privatus tinklas** (angl. *virtual private network VPN*) – atskirų nutolusių vienas nuo kito kompiuterių sujungimas į vieną saugų tinklą internetu.

4. Kitos sąvokos atitinka 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“, vartojamas sąvokas.

5. DSAIS duomenys nėra klasifikuojami ar skirstomi į duomenų kategorijas.

6. DSAIS tvarkomos elektroninės informacijos sąrašas nurodytas Valstybinės kainų ir energetikos kontrolės komisijos duomenų surinkimo ir analizės informacinės sistemos nuostatų, patvirtintų Komisijos pirmininko 2013 m gegužės 7 d. įsakymu Nr. O1-40 „Dėl Valstybinės kainų ir energetikos kontrolės komisijos duomenų surinkimo ir analizės informacinės sistemos įsteigimo ir jos nuostatų patvirtinimo bei duomenų surinkimo ir analizės informacinės sistemos duomenų saugos nuostatų patvirtinimo“, IV skyriuje.

7. DSAIS duomenys neperkeliami ir neteikiami kitoms informacinėms sistemoms.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

8. DSAIS įranga prižiūrima laikantis gamintojo rekomendacijų. Įrangą prižiūri ir gedimus šalina kvalifikuoti specialistai.

9. DSAIS perspėja DSAIS administratorių, kai pagrindinėje DSAIS techninėje įrangoje sumažėja iki nustatytos pavojingos ribos laisvos techninės įrangos atminties ar vietos diske, ilgą laiką labai apkraunamas centrinis procesorius ar duomenų perdavimo tinklo sąsaja.

10. DSAIS naudoja tik legalią programinę įrangą.

11. DSAIS saugumui užtikrinti naudojama programinė įranga efektyviai apsaugo nuo kenksmingo kodo programų (antivirusinė programinė įranga, nepageidaujamo turinio valdymo įranga ir pan.). Antivirusinės programinės įrangos kenksmingo kodo aprašai atnaujinami ne rečiau kaip kartą per 24 valandas.

12. Operatyviai įdiegiami prieš tai patikrinti DSAIS operacinės sistemos ir naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;

13. DSAIS duomenų perdavimo tinklas atskirtas nuo viešųjų telekomunikacijų tinklų užkarda.

14. DSAIS saugumui užtikrinti naudojamos lokalios programinės ir duomenų perdavimo tinklo užkardos. Konfigūruojant užkardas laikomasi principo „draudžiama viskas, išskyrus“, t. y. DSAIS leidžiamas tik būtinas darbui duomenų perdavimo tinklo srautas.

15. Už duomenų perdavimo tinklo užkardų priežiūrą, užkardos valdymo sistemos priežiūrą ir tinkamą užkardų sąranką atsakingas DSAIS administratorius.

16. Užkardų konfigūracijos aprašymą rengia jų administratorius. Konfigūracijos aprašymą saugo saugos įgaliotinis. Užkardų konfigūracija tikrinama ne rečiau kaip kartą per metus, tikrinimą organizuoja saugos įgaliotinis.

17. Viešaisiais telekomunikaciniais tinklais perduodamos informacinės sistemos elektroninės informacijos konfidencialumas užtikrinamas naudojant šifravimą, virtualų privatų tinklą (angl. *virtual private network*), skirtines linijas, saugų valstybinį duomenų perdavimo tinklą ir kitas priemones.

18. Apribota fizinė prieiga prie DSAIS tarnybinių stočių. DSAIS tarnybinės stotys yra nuotoliniame duomenų centre (toliau – DC), kuris sertifikuotas ISO 27001 ir atitinka keliamus reikalavimus:

18.1. patekimo į duomenų centro teritoriją tvarka aprašyta paslaugų teikėjo vidinėje tvarkoje „Informacijos saugumo vadovas“;

18.2. DC patalpos visą parą saugomos pasitelkiant signalizacijos sistemą ir rakinamos elektroniniu raktu;

18.3. patalpų įeigos korteles su sukurtais unikaliais signalizacijos kodais turi tik darbuotojai, prižiūrintys duomenų centrą. Jokie pašaliniai asmenys, išskyrus turinčius įeigos į duomenų centrą korteles, neturi teisės patekti į DC patalpas;

18.4. rangovai, aptarnaujantis personalas į DC patalpas gali patekti tik lydint DC prižiūrinčiam darbuotojui.

19. DSAIS tarnybinių stočių patalpoje yra:

19.1. įdiegtos sistemos, leidžiančios informuoti atsakingus darbuotojus apie DC infrastruktūros – elektros linijų būklės, generatoriaus būsenos, kondicionierių gedimų, duomenų centro aplinkos – parametrus;

19.2. elektros srovės nepertraukiamas tiekimas DC laikomoms DSAIS tarnybinėms stotims užtikrinamas pasitelkiant nepertraukiamo maitinimo šaltinio sistemą;

19.3. dingus elektrai ilgesniam laikui, automatiškai įsijungia autonominis elektros srovės generatorius, užtikrinantis nepertraukiamą duomenų centre esančių tarnybinių stočių veikimą esant maksimaliai jo apkrovai;

19.4. DC patalpose įrengta klimato kontrolės sistema, kondicionierių gedimai stebimi dedikuotu aparatiniu monitoringo įrenginiu;

19.5. pastate, kuriame įkurtas DC, įrengta video- stebėjimo sistema, apsaugos ir gaisro signalizacijos. Apsaugos poste budi saugos įmonės darbuotojas.

20. Registruojami ir ne mažiau kaip 30 kalendorinių dienų saugomi duomenys apie DSAIS įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis DSAIS, kitus saugai svarbius įvykius su nuoroda į DSAIS naudotojo identifikatorių ir įvykio laiką. Ši informacija reguliariai analizuojama.

21. Daromos atsarginės elektroninės informacijos kopijos laikomos atskiroje patalpoje. Už DSAIS duomenų kopijavimą, saugojimą ir atkūrimą atsako DSAIS tarnybinių stočių talpinimo paslaugų teikėjas. Siekiant užtikrinti DSAIS veiklos tęstinumą, sistemos tarnybinės stotys dubliuojamos.

22. Atsarginių elektroninės informacijos kopijų darymas fiksuojamas žurnale.

23. Visuose DSAIS vidinių naudotojų kompiuteriuose įdiegtos ekrano užsklandos (angl. *screen saver*). Jos apsaugotos slaptažodžiu (režimo aktyvavimo laikas – ne daugiau 10 minučių).

24. DSAIS vidiniai naudotojai, trumpam palikdami savo darbo vietą, privalo užrakinti savo kompiuterį (angl. *lock computer*).

25. Baigę darbą DSAIS vidiniai naudotojai privalo uždaryti visas programas, išimti ir į stalčių sudėti duomenų laikmenas, atsijungti nuo savo paskyros.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

26. Saugus elektroninės informacijos keitimo, atnaujinimo, įvedimo ir naikinimo užtikrinimo tvarka:

26.1. DSAIS duomenis įvesti, keisti, atnaujinti ir naikinti gali tik DSAIS administratorius;

26.2. DSAIS administruoti ataskaitų šablonus, formų šablonus, prižiūrėti ataskaitų pateikimo terminus, tvarkyti darbo sekas gali DSAIS ataskaitų administratorius ir DSAIS administratorius;

26.3. DSAIS tam tikrus duomenis peržiūrėti ataskaitų darbo sekose gali DSAIS vidinis naudotojas, DSAIS ataskaitų administratorius ir DSAIS administratorius.

27. Duomenys į DSAIS duomenų bazes gali būti įvesti, atnaujinami, naikinami tik turint teisėtą pagrindą.

28. DSAIS registruoja duomenų pakeitimus atlikusius DSAIS naudotojus ir duomenų keitimo laiką. Registruojami ir ne mažiau kaip 30 kalendorinių dienų saugomi duomenys apie DSAIS

įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis DSAIS, kitus saugai svarbius įvykius su nuoroda į DSAIS naudotojo identifikatorių ir įvykio laiką. Ši informacija reguliariai analizuojama.

29. Saugomi duomenys apie DSAIS naudotojo veiksmus DSAIS. Duomenys saugomi registruojančios programinės įrangos gamintojų numatytą laiką. Daromos atsarginės elektroninės informacijos kopijos, kurios laikomos atskiroje patalpoje. Už DSAIS duomenų kopijavimą, saugojimą ir atkūrimą atsako DSAIS administratorius. Siekiant užtikrinti DSAIS veiklos tęstinumą, sistemos tarnybinės stotys dubliuojamos.

30. DSAIS turi įvestos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemones.

31. DSAIS registruoja bent vieną paskutinį informacinės sistemos elektroninės informacijos pakeitimą atlikusį informacinės sistemos naudotoją ir pakeitimo laiką.

32. Elektroninė informacija kopijose yra užšifruota arba imtasi kitų priemonių, neleidžiančių panaudoti kopijų elektroninei informacijai neteisėtai atkurti.

33. Atsarginių elektroninės informacijos kopijų darymas fiksuojamas elektroniniame žurnale.

34. DSAIS prižiūrima naudojant atskirą tam skirtą DSAIS administratoriaus prieigą, kuria naudojantis negalima atlikti informacinės DSAIS naudotojo funkcijų.

35. Techninės įrangos, operacinių sistemų ir taikomosios programinės įrangos keitimai ir naujinimai yra valdomi:

35.1. esminiai keitimai ir naujinimai identifikuojami ir registruojami;

35.2. keitimai ir naujinimai planuojami ir testuojami;

35.3. įvertinama susijusi su keitimų ir naujinimų poveikiu rizika, įskaitant poveikį saugumui;

35.4. numatyta formali keitimų ir naujinimų tvirtinimo procedūra;

35.5. su informacija apie keitimus ir naujinimus supažindintos visos susijusios šalys (DSAIS naudotojai, DSIAS administratorius, DSAIS ataskaitų administratorius, saugos įgaliotinis ir kt.);

35.6. numatytos atstatomosios / grįžtamosios procedūros nesėkmingų keitimų ar naujinimų atvejams.

IV SKYRIUS
REIKALAVIMAI, KELIAMI PERKAMŲ INFORMACINIŲ SISTEMŲ FUNKCIONAVIMUI, REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

36. Siekiant praplėsti DSAIS funkcionuoti reikalingas paslaugas, prireikus gali būti pasitelkiami išorės tiekėjai, sudarant su jais atitinkamas paslaugų teikimo sutartis.

37. DSAIS administratorius atsako už programinių, techninių ir kitų prieigos prie DSAIS resursų organizavimą, suteikimą ir panaikinimą techninės ir (ar) programinės paslaugos teikėjui.

38. DSAIS administratorius suteikia paslaugas teikėjui tik tokią prieigą prie DSAIS resursų, kuri yra būtina norint vykdyti sutartyje nustatytus įsipareigojimus, kurie neprieštarauja įstatymų ir kitų teisės aktų reikalavimams.

39. Su tiekėju turi būti suderinta paslaugos teikimo tvarka, į kurią įtraukti prieigos reikalavimai bei jų suteikimo sąlygos.

40. Pasibaigus sutarties su paslaugos teikėjais galiojimo terminui ar atsiradus kitoms sutartyje ar saugos politiką įgyvendinančiuose dokumentuose įvardytoms sąlygoms, DSAIS administratorius nedelsdamas privalo panaikinti suteiktą prieigą.

41. Reikalavimai, keliami teikėjų patalpoms, įrangai, DSAIS priežiūrai, duomenų perdavimo tinklams ir kitoms paslaugoms, nurodomi DSAIS taikomosios programinės įrangos paslaugų teikimo sutartyse.

42. Tiekėjų darbuotojams, atliekantiems administravimo funkcijas, taikomi visi atitinkamo lygio DSAIS administratoriams DSAIS naudotojų administravimo taisyklėse ir DSAIS saugaus elektroninės informacijos tvarkymo taisyklėse nustatyti reikalavimai.

43. Perkant ar nuomojant techninę ar programinę įrangą turi būti atsižvelgiama į:

43.1. atitiktį DSAIS keliamiems saugos reikalavimams;

43.2. turimos įrangos suderinamumą su planuojama įsigyti duomenų kopijavimo ir atsarginio kopijavimo įranga;

43.3. suderinamumą su turima stebėsenos sistema, leidžiančia informuoti apie įrangos, aplinkos, duomenų perdavimo ir elektros tinklų bei kitus kritinius pokyčius.

44. Sutartyse su trečiosiomis šalimis, susijusiomis su Komisijos informacijos ar informacijos apdorojimo priemonių prieiga, duomenų apdorojimu, perdavimu ar valdymu, yra numatytas reikalavimas pasirašyti konfidencialumo susitarimą ir laikytis DSAIS saugos reikalavimų.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

45. DSAIS naudotojai, DSAIS ataskaitų administratoriai privalo kaip galima greičiau informuoti saugos įgaliotinį ir DSAIS administratorių apie pastebėtus Taisyklių reikalavimų pažeidimus, DSAIS veiklos sutrikimus arba neįprastą DSAIS veikimą.

46. Taisyklės privalomos visiems DSAIS naudotojams, DSAIS administratoriui, DSAIS ataskaitų administratoriui ir saugos įgaliotiniui.

47. Saugos įgaliotinis, DSAIS administratorius, DSAIS ataskaitų administratorius, DSAIS naudotojai, pažeidę Taisyklių, Valstybinės kainų ir energetikos kontrolės komisijos duomenų surinkimo ir analizės informacinės sistemos duomenų saugos nuostatus, patvirtintus Komisijos pirmininko 2013 m. gegužės 7 d. įsakymu Nr. O1-40 „Dėl Valstybinės kainų ir energetikos kontrolės komisijos duomenų surinkimo ir analizės informacinės sistemos įsteigimo ir jos nuostatų patvirtinimo bei duomenų surinkimo ir analizės informacinės sistemos duomenų saugos nuostatų patvirtinimo“ ar kitų DSAIS saugos politiką reguliuojančių teisės aktų reikalavimus, atsako šių Taisyklių ir Lietuvos Respublikos įstatymų nustatyta tvarka.

_____