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

VALSTYBINĖS KAINŲ IR ENERGETIKOS KONTROLĖS KOMISIJOS ELEKTROS ENERGIJOS KAINŲ PALYGINIMO INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės kainų ir energetikos kontrolės komisijos (toliau – Komisija) elektros energijos kainų palyginimo informacinės sistemos (toliau – Sistemos) saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) nustato tvarką, pagal kurią turi būti saugiai tvarkoma Sistemos 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, patvirtintais 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. Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais 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. Komisijos Sistemos ir Sistemos duomenų saugos nuostatais, patvirtintais Komisijos pirmininko 2015 m. balandžio 20 d. įsakymu Nr. O1-39 „Dėl elektros energijos kainų palyginimo informacinės sistemos nuostatų ir elektros energijos kainų palyginimo informacinės sistemos duomenų saugos nuostatų patvirtinimo“ (toliau – Sistemos duomenų saugos nuostatai);

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 Sistemoje;

3.2. **Sistemos administratorius** – Komisijos paskirtas valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, administruojantis Komisijos vietinio tinklo aktyviąją įrangą, užtikrinantis tarnybinių stočių, elektroninio pašto, Komisijoje naudojamų informacinių sistemų operacinių sistemų ir taikomosios programinės įrangos priežiūrą, administravimą, saugią eksploataciją ir/arba išorės tiekėjas, su kuriuo sudaryta Sistemos priežiūros paslaugų teikimo sutartis;

3.3. **Sistemos išorinis naudotojas** – Ūkio subjektas (Ūkio subjekto atstovas), kuris naudojasi Sistema duomenų teikimui ir kitiems susijusiems veiksmams atlikti;

3.4. **Sistemos vidinis administratorius** – Komisijos įsakymu paskirtas valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį, Sistemoje turintis aukščiausio lygio teises, vykdantis Sistemos išorinių naudotojų teisių ir duomenų tvarkymo priežiūrą;

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

3.6. **Sistemos naudotojas** – Sistemos vidinis administratorius arba išorinis naudotojas;

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

4. Kitos Taisyklėse naudojamos 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. Sistemos duomenys nėra klasifikuojami ar skirstomi į duomenų kategorijas.

6. Sistemos tvarkomos elektroninės informacijos sąrašas nurodytas Sistemos duomenų saugos nuostatų II skyriuje.

7. Sistemos duomenų perkėlimas ir teikimas kitoms informacinėms sistemoms nevykdomas.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

8. Sistemos įranga yra prižiūrima, laikantis gamintojo rekomendacijų. Įrangos priežiūrą ir gedimų šalinimą atlieka kvalifikuoti specialistai.

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

10. Sistema naudoja tik legalią programinę įrangą.

11. Sistemos 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 yra atnaujinami ne rečiau kaip kartą per 24 valandas.

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

13. Sistemos duomenų perdavimo tinklas yra atskirtas nuo viešųjų telekomunikacijų tinklų užkarda.

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

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

16. Užkardų konfigūracijos aprašymą rengia jų administratorius. Konfigūracijos aprašymas saugomas pas Saugos įgaliotinį. Užkardų konfigūracija tikrinama ne rečiau kaip kartą per metus, tikrinimą organizuoja Saugos įgaliotinis.

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

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

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

18.2. DC patalpos visą parą saugomos signalizacijos sistema ir rakinamos elektroninio rakto pagalba;

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

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

19. Sistemos 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 Sistemos tarnybinėms stotims užtikrinamas nepertraukiamo maitinimo šaltinio sistemos pagalba;

19.3. dingus elektrai ilgesniam laikui, automatiškai įsijungia autonominis elektros srovės generatorius, užtikrinantis nepertraukiamą duomenų centre talpinamų tarnybinių stočių veikimą esant maksimaliam jo apkrovimui;

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

19.5. pastate, kuriame įkurtas DC, yra 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 Sistemos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis Sistemoje, kitus saugai svarbius įvykius, su nuoroda į Sistemos naudotojo identifikatorių ir įvykio laiką. Ši informacija yra reguliariai analizuojama.

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

22. Atsarginių elektroninės informacijos kopijų darymas yra fiksuojamas žurnale.

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

24. Sistemos administratoriai ir Sistemos vidiniai administratoriai trumpam palikdami savo darbo vietą privalo užrakinti savo kompiuterį (angl. *lock computer*).

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

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

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

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

26.2. Sistemos išorinių naudotojų paskyras, vidinius nustatymus gali administruoti Sistemos administratorius ir Sistemos vidinis administratorius;

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

28. Sistema registruoja duomenų pakeitimus atlikusius Sistemos naudotojus ir duomenų keitimo laiką. Registruojami ir ne mažiau kaip 30 kalendorinių dienų saugomi duomenys apie Sistemos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis Sistemoje, kitus saugai svarbius įvykius, su nuoroda į Sistemos naudotojo identifikatorių ir įvykio laiką. Ši informacija yra reguliariai analizuojama.

29. Reguliariai daromos atsarginės Sistemos tarnybinės stoties duomenų kopijos, kurios laikomos atskiroje patalpoje. Už Sistemos duomenų kopijavimą, saugojimą ir atkūrimą atsako talpinimo paslaugos ir sistemos priežiūros paslaugos tiekėjas. Siekiant užtikrinti Sistemos veiklos tęstinumą, sistemos tarnybinės stotys yra dubliuojamos.

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

31. Sistema registruoja bent vieną paskutinį Sistemos elektroninės informacijos pakeitimą atlikusį Sistemos naudotoją ir pakeitimo laiką.

32. Elektroninė informacija kopijose yra užšifruota arba imtasi kitų priemonių, neleidžiančių panaudoti kopijų neteisėtam elektroninės informacijos atkūrimui.

33. Atsarginių elektroninės informacijos kopijų darymas yra fiksuojamas elektroniniame žurnale.

34. Sistemos priežiūros funkcijos yra atliekamos, naudojant atskirą tam skirtą Sistemos administratoriaus prieigą, kuria naudojantis nėra galima atlikti Sistemos 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 yra supažindintos visos susijusios šalys (Sistemos naudotojai, Sistemos administratorius, Saugos įgaliotinis ir kt.);

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

35.7. Nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių naudojimo tvarką Komisijoje nustato Valstybinės kainų ir energetikos kontrolės komisijos kompiuterių ir programinės įrangos diegimo tvarkoje, patvirtintoje 2013 m. spalio 17 d. Komisijos pirmininko įsakymu Nr. O1-85 „Dėl Valstybinės kainų ir energetikos kontrolės komisijos naudojamų kompiuterių ir programinės įrangos diegimo ir eksploatavimo tvarkos aprašo“

IV SKYRIUS
REIKALAVIMAI SISTEMOS FUNKCIONAVIMUI, REIKALINGOMS PASLAUGOMS ĮSIGYTI IR JŲ TEIKĖJAMS

36. Prireikus Sistemai funkcionuoti reikalingoms paslaugoms praplėsti gali būti pasitelkiami išorės tiekėjai, sudarant su jais atitinkamas paslaugų teikimo sutartis.

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

38. Sistemos administratorius suteikia paslaugas teikėjui tik tokia prieiga prie Sistemos resursų, kuri yra būtina norint atlikti arba vykdyti sutartyje nustatytus įsipareigojimus, kurie neprieštarauja įstatymų ir kitų teisės aktų reikalavimams.

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

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

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

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

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

43.1. atitikimą Sistemai 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 Sistemos saugos reikalavimų.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

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

46. Taisyklės yra privalomos visiems Sistemos naudotojams, Sistemos administratoriui ir Saugos įgaliotiniui.

47. Saugos įgaliotinis, Sistemos administratorius, Sistemos naudotojai, pažeidę Taisyklių, Sistemos Duomenų saugos nuostatų ar kitų Sistemos saugos politiką reguliuojančių teisės aktų reikalavimus, atsako šių Taisyklių ir Lietuvos Respublikos įstatymų nustatyta tvarka.

_____