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 NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės kainų ir energetikos kontrolės komisijos (toliau – Komisija) elektros energijos kainų palyginimo informacinės sistemos (toliau – Sistema) naudotojų administravimo taisyklės
(toliau – Taisyklės) nustato naudotojų prieigos prie Sistemos valdymą, užtikrinant informacijos saugumą.

2. Taisyklės taikomos visiems Sistemos naudotojams ir Saugos įgaliotiniui.

3. Sistemos naudotojai turi turėti tik tiek priėjimo prie Sistemos teisių, kiek būtina jų tiesioginėms funkcijoms vykdyti.

4. Prieinamumas prie Sistemos duomenų naudotojams suteikiamas, vadovaujantis principu „būtina žinoti“, t. y. asmeniui gali būti patikėta tokios apimties informacija, kokios reikia jo pareigoms atlikti.

5. Taisyklės parengtos vadovaujantis:

5.1. 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“;

5.2. 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“;

5.3. 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);

5.4. 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.

6. Taisyklėse vartojamos sąvokos:

6.1. **Sistemos valdytojas** – Komisija

6.2. **Saugos įgaliotinis** – Sistemos valdytojo paskirtas valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį, koordinuojantis ir prižiūrintis saugos politikos įgyvendinimą Sistemoje;

6.3. **Sistemos administratorius** – Sistemos valdytojo paskirtas valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, administruojantis Sistemos valdytojo vietinio tinklo aktyviąją įrangą, užtikrinantis tarnybinių stočių, elektroninio pašto, Sistemos valdytojo 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;

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

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

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

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

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

7. 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.

II SKYRIUS
SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS TVARKA

8. Saugos įgaliotinis organizuoja Sistemos naudotojų susipažinimą su Sistemos valdytojo patvirtintais Sistemos Duomenų saugos nuostatais, Saugaus elektroninės informacijos tvarkymo taisyklėmis ir šiomis Taisyklėmis.

9. Sistemos naudotojai supažindinami su saugos dokumentais šiais atvejais:

9.1. prieš suteikiant naudotojams prieigą prie Sistemos;

9.2. pakeitus saugos politiką reglamentuojančius ir įgyvendinančius dokumentus;

9.3. periodiškai informacijos saugos mokymų metu, ne rečiau kaip kartą per 2 metus.

10. Supažindinimo su saugos dokumentais formą saugos įgaliotinis nustato savo nuožiūra, atsižvelgdamas į šias rekomendacijas:

10.1. jei supažindinamas vienas naudotojas, leisti naudotojui su dokumentais susipažinti savarankiškai ir susitikimo metu įsitikinti, ar dokumentų turinys buvo tinkamai suprastas (užduoti klausimų);

10.2. jei supažindinama grupė naudotojų, surengti trumpą seminarą, kurio metu būtų pristatomi saugos dokumentai, apžvelgiamas jų turinys, užduodami klausimai naudotojams ir atsakoma į naudotojams iškilusius klausimus.

III SKYRIUS
SAUGAUS DUOMENŲ TEIKIMO SISTEMOS NAUDOTOJAMS KONTROLĖS TVARKA

11. Sistemos naudotojų tapatybei nustatyti Sistemos administratorių, Sistemos vidinių administratorių ir Sistemos išorinių naudotojų atveju taikomi skirtingi algoritmai ir reikalavimai:

11.1. Sistemos administratorių ir Sistemos vidinių administratorių atveju – su Sistema gali dirbti tik Sistemos valdytojo pirmininko įsakymu paskirtas valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį;

11.2. Sistemos išorinių naudotojų atveju – registruotis ir dirbti su Sistema galima tik per Elektroninius valdžios vartus nustačius asmens tapatybę, pasinaudojant elektroninės bankininkystės sistema, elektroniniu parašu ar asmens tapatybės kortele.

12. Reikalavimai Sistemos administratorių ir Sistemos vidinių administratorių pasijungimui prie Sistemos:

12.1. sistemos administratorius jungtis prie Sistemos gali tik iš jam suteiktos darbo vietos, vidiniame Komisijos tinkle; prisijungimas prie Sistemos iš išorinio tinklo nėra galimas;

12.2. sistemos vidinis administratorius jungtis prie Sistemos, jam suteiktomis teisėmis, gali tik su jam Sistemoje priskirtu vartotojo vardu ir slaptažodžiu.

13. Reikalavimai Sistemos administratorių ir Sistemos vidinių administratorių kompiuterinių darbo vietų slaptažodžių sudarymui, galiojimo trukmei:

13.1. slaptažodis turi būti sudarytas iš ne mažiau kaip 12 simbolių kombinacijos, t. y. lotyniškos abėcėlės mažųjų, didžiųjų raidžių, skaitmenų, specialiųjų simbolių;

13.2. slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija;

13.3. draudžiama slaptažodžius atskleisti tretiesiems asmenims;

13.4. slaptažodžiai nėra saugomi ir perduodami atviru tekstu, išskyrus atvejus, kai saugos įgaliotinio sprendimu yra perduodamas laikinas slaptažodis pasijungimui prie kompiuterinės darbo vietos;

13.5. slaptažodžiai keičiami ne rečiau kaip kas 60 kalendorinių dienų;

13.6. keičiant slaptažodį informacinės sistemos taikomoji programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių 3 paskutinių slaptažodžių;

13.7. didžiausias leistinas mėginimų skaičius įvesti teisingą slaptažodį yra 5 kartai; neteisingai įvedus didžiausią leistiną skaičių, Sistema užsiblokuoja ir neleidžia naudotojui identifikuotis ir prisijungti prie Sistemos, naudotoją naujai aktyvuoti galima tik susisiekus su Sistemos administratoriumi.

14. Reikalavimai Sistemos išorinių naudotojų pasijungimui prie Sistemos:

14.1. Sistemos išorinis naudotojas gali visada jungtis prie Sistemos, naudodamasis Elektroninių valdžios vartų paslauga arba registracijos metu nurodytu el. pašto adresu bei sudarytu slaptažodžiu;

14.2. Sistemos išorinis naudotojas, nustatęs ir patvirtinęs savo tapatybę, naudodamasis Elektroninių valdžios vartų paslauga, nukreipiamas į registracijos formą, kurioje nurodo Ūkio subjekto informaciją ir prisijungimui skirtą el. pašto adresą bei paskyros slaptažodį;

14.3. Sistemos išorinio naudotojo slaptažodis turi būti sudarytas iš ne mažiau kaip 8 simbolių kombinacijos, t. y. lotyniškos abėcėlės mažųjų, didžiųjų raidžių, skaitmenų, specialiųjų simbolių;

14.4. draudžiama slaptažodžius atskleisti tretiesiems asmenims;

14.5. Sistemos išorinių naudotojų slaptažodžiai nėra saugomi ir perduodami atviru tekstu;

14.6. Sistemos išorinis naudotojas prie Sistemos jungiasi identifikuodamas savo tapatybę per Elektroninius valdžios vartus. Didžiausias leistinas mėginimų skaičius įvesti teisingą slaptažodį yra 5 kartai; neteisingai įvedus didžiausią leistiną skaičių, Sistema užsiblokuoja ir neleidžia naudotojui identifikuotis ir prisijungti prie Sistemos. Sistemos išorinis naudotojas negalėdamas prisijungti prie Sistemos ar pamiršęs prisijungimo slaptažodį, gali kreiptis raštu į Sistemos valdytoją dėl naujo slaptažodžio suteikimo.

15. Prieigos teisė prie Sistemos arba jos dalies panaikinama, jeigu:

15.1. Sistemos administratoriaus ir Sistemos vidinio administratoriaus atveju:

15.1.1. naudotojas atleidžiamas iš valstybės tarnybos ar darbo;

15.1.2. naudotojas keičia darbo vietą (pareigybę);

15.1.3. naudotojo tiesioginis vadovas pateikia prašymą dėl prieigos parametrų pakeitimo arba panaikinimo;

15.1.4. nustatomas naudotojo neteisėtas duomenų naudojimas;

15.1.5. Sistemos valdytojui kyla įtarimų, kad naudotojas piktnaudžiauja suteiktomis prieigos teisėmis ir gali pažeisti Sistemos arba joje apdorojamų duomenų saugumą;

15.1.6. pasibaigia/nutraukiama Sistemos priežiūros paslaugų sutartis su tiekėju, kuris atlieka Sistemos priežiūros ir palaikymo funkcijas.

15.2. Sistemos išorinių naudotojų atveju:

15.2.1. Ūkio subjektas raštu kreipiasi į Sistemos valdytoją, pateikdamas prašymą dėl prieigos parametrų pakeitimo arba panaikinimo;

15.2.2. nustatomas Sistemos išorinio naudotojo neteisėtas duomenų naudojimas;

15.2.3. Sistemos administratoriui arba Sistemos vidiniam administratoriui kyla įtarimų, kad Sistemos išorinis naudotojas piktnaudžiauja suteiktomis prieigos teisėmis ir gali pažeisti Sistemos arba joje apdorojamų duomenų saugumą. Kilus tokiems įtarimams, Sistemos administratorius arba Sistemos vidinis administratorius raštu kreipiasi į saugos įgaliotinį leidimo panaikinti naudotojo prieigos teisę. Sistemos administratorius arba Sistemos vidinis administratorius privalo pagrįsti įtarimus. Saugos įgaliotiniui leidus panaikinti Sistemos naudotojo prieigą, Sistemos administratorius arba Sistemos vidinis administratorius apie tai informuoja Ūkio subjektą.

16. Prisijungimai ir (ar) bandymai prisijungi prie Sistemos automatiniu būdu įrašomi Sistemos duomenų bazės veiksmų žurnale, kuriame registruojami prisijungimo ir (ar) bandymo prisijungti data, laikas, prisijungimo trukmė, prisijungiančio Sistemos naudotojo vardas ir kompiuterio, iš kurio prisijungiama IP adresas, Sistemos funkcijos, prie kurių buvo jungtasi, atlikti veiksmai su duomenimis (įvedimas, peržiūra, keitimas, naikinimas ir kiti duomenų tvarkymo veiksmai). Šie įrašai saugomi ne trumpiau kaip 1 metus.

IV SKYRIUS
SISTEMOS NAUDOTOJŲ IR ADMINISTRATORIŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

17. Sistemos naudotojai gali naudotis tik tomis Sistemos dalimis ir jose apdorojamais duomenimis, prie kurių prieiga jiems yra numatyta pagal pareigas, ir kurią suteikė Sistemos valdytojas.

18. Sistemos naudotojai privalo užtikrinti Sistemos ir joje apdorojamų duomenų konfidencialumą, vientisumą ir prieinamumą, vadovaudamiesi šiose Taisyklėse nustatytais reikalavimais.

19. Prieš pradedant naudotis Sistema, Sistemos naudotojas ir Sistemos administratorius privalo susipažinti su visais Sistemos valdytojo informacijos saugą reglamentuojančiais ir įgyvendinančiais dokumentais:

19.1. supažindinimas Sistemos administratoriui (išskyrus išorės tiekėją) ir Sistemos vidiniam administratoriui pateikiamas elektronine forma per dokumentų valdymo sistemą (DVS), taip patvirtinant savo sutikimą vykdyti visus minėtų dokumentų reikalavimus;

19.2. Sistemos išoriniai naudotojai privalo susipažinti su saugos politiką reguliuojančiais teisės aktais ir instrukcijomis. Informacija apie Saugos politiką įgyvendinančius teisės aktų ir jų pasikeitimus viešai skelbiama tinklalapyje www.regula.lt

20. Sistemos vidiniams administratoriams ir Sistemos administratoriams draudžiama:

20.1. leisti kitiems asmenimis naudotis jiems paskirta technine įranga ar savo prieigos vardu, nebent tam yra objektyvių priežasčių (pvz., technine įranga dirba keli asmenys);

20.2. savavališkai keisti bei ardyti techninės įrangos ar jos sudėtinių dalių, jungti prie vidaus duomenų perdavimo tinklo kitą (pvz., asmeninę) techninę įrangą;

20.3. patiems diegti, konfigūruoti ar trinti programinę įrangą, keisti operacinės sistemos parametrus savo kompiuteriuose (išskyrus Sistemos administratorius, šiems atliekant su darbu susijusias užduotis);

20.4. techninėje įrangoje diegti ir naudoti nelegalią programinę įrangą bei audiovizualinius įrašus. Naudotojams taip pat yra draudžiama kopijuoti Sistemos valdytojo įsigytą licencijuotą programinę įrangą, ją platinti ar naudoti asmeniniais tikslais kitaip, negu tai numato licencinė sutartis;

20.5. sąmoningas kenksmingo kodo platinimas;

20.6. parsisiųsdinti iš interneto ir platinti autorių teisių saugomą bei licencijuojamą programinę įrangą, vaizdo ir garso įrašus bei elektronines knygas, pažeidžiant Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymą;

20.7. jungtis prie vidaus duomenų perdavimo tinkle esančių serverių ir juose saugomos informacijos (išskyrus Sistemos administratorius, šiems atliekant su darbu susijusias užduotis);

20.8. siųsti, gauti (užsisakius atsiuntimą) ar persiųsti elektroninių rinkmenų, nesusijusių su darbo funkcijomis (pvz., žaidimų, vaizdo bei garso rinkmenų ir kt.).

21. Jei tam tikra programinė įranga yra reikalinga Sistemos vidiniam administratoriui jo darbo užduotims atlikti, jo skyriaus vadovas privalo pateikti Sistemos administratoriui raštišką prašymą, kuriame turi pagrįsti programinės įrangos reikalingumą ir nurodyti, kokias funkcijas programinė priemonė turėtų atlikti. Gavęs prašymą Sistemos administratorius sprendžia, ar programinę priemonę realizuoti Sistemos valdytojo pajėgomis ar pirkti viešojo pirkimų konkurso būdu.

22. Jeigu Sistemos naudotojas turi įtarimų, kad jo naudojama techninė įranga yra paveikta (užkrėsta) kenksmingo kodo (virusu), jis nedelsdamas privalo nutraukti naudojimąsi šia įranga ir informuoti apie tai atsakingus informacinių technologijų specialistus. Duomenų laikmenos, naudojamos šiame kompiuteryje, negali būti naudojamos bet kurioje kitoje sistemoje iki kol kenksmingas kodas bus veiksmingai sunaikintas. Naudotojui draudžiama mėginti sunaikinti kenksmingą kodą pačiam – tai atlieka atsakingi informacinių technologijų specialistai.

23. Sistemos naudotojas būtinai nedelsdamas turi pakeisti prisijungimo slaptažodį, jeigu įtaria, kad jo slaptažodį sužinojo kitas asmuo.

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

25. Naudotojai, dėl Sistemos sutrikimų, neįprasto jų veikimo, esamų arba galimų informacijos saugumo reikalavimų pažeidimų ar kitų naudotojų nederamų veiksmų, nedelsdami privalo kreiptis į Sistemos saugos įgaliotinį arba Sistemos administratorių.

26. Naudotojai iš Sistemos administratorių turi teisę reikalauti užtikrinti deramą jų naudojamos Sistemos ir joje apdorojamų duomenų saugumo lygį, gauti informaciją apie taikomas saugos priemones ir rekomenduoti papildomas saugos priemones.

27. Leistini nuotolinio prisijungimo būdai:

27.1. nuotoliniam prisijungimui prie Sistemos išoriniams naudotojams papildomi reikalavimai nekeliami;

27.2. nuotolinis Sistemos administratorių prisijungimas prie Sistemos tarnybinių stočių galimas tik naudojantis VPN tuneliu;

27.3. bandymų prisijungti prie Sistemos automatiniu būdu skaičius įrašomas Sistemos duomenų bazės veiksmų žurnale, kuriame registruojami prisijungimo ir (ar) bandymo prisijungti data, laikas, ir prisijungiančio Sistemos naudotojo vardas.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

28. Taisyklių laikymąsi prižiūri ir patikrinimus organizuoja Saugos įgaliotinis, kartą į metus pasirinkdamas kontrolinę Sistemos naudotojų grupę.

29. Sistemos Saugos įgaliotinis, administratorius, 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.

_____