P A T V I R T I N T A
Valstybinės kainų ir energetikos
kontrolės komisijos pirmininko
2015 m. įsakymu Nr. O1-

ELEKTROS ENERGIJOS KAINŲ PALYGINIMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Elektros energijos kainų palyginimo informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Valstybinės kainų ir energetikos kontrolės komisijos informacinės sistemos duomenų saugą ir nustato jų saugos politiką (toliau – Saugos politika).

2. Saugos nuostatų tikslas nustatyti technines ir organizacines priemones, kurios leistų užtikrinti elektroninės informacijos, saugomos ir apdorojamos Elektros energijos kainų palyginimo informacinės sistemos (toliau – Sistema) konfidencialumą, prieinamumą, vientisumą ir tinkamą kompiuterizuotų darbo vietų bei kompiuterių tinklo aktyvios įrangos funkcionavimą. Sistemoje duomenų saugai užtikrinti privaloma kompleksiškai naudoti administracines, technines ir programines priemones, padedančias įgyvendinti reagavimo, atsakomybės, elektroninės informacijos saugos suvokimo stiprumo bei saugos priemonių projektavimo ir diegimo principus.

3. Šie Saugos nuostatai parengti vadovaujantis Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, kitais teisės aktais. Saugos nuostatuose vartojamos sąvokos atitinka šiuose teisės aktuose ir Lietuvos standarte LST ISO/IEC 27002:2009 vartojamas sąvokas.

4. Informacijos saugumo užtikrinimo prioritetinės kryptys:

4.1. elektroninės informacijos konfidencialumo užtikrinimas;

4.2. elektroninės informacijos vientisumo užtikrinimas;

4.3. elektroninės informacijos prieinamumo užtikrinimas;

4.4. Sistemos veiklos tęstinumas;

5. Sistemos valdytoja ir tvarkytoja yra Valstybinė kainų ir energetikos kontrolės komisija (toliau – VKEKK, Valdytojas arba Tvarkytojas), Verkių g. 25C-1, LT-08223 Vilnius.

6. Sistemos Valdytojo vadovo funkcijos ir atsakomybė:

6.1. organizuoja Sistemos veiklą ir jai vadovauja, paveda Sistemos Tvarkytojui skirti Sistemos saugos įgaliotinį;

6.2. rengia ir tvirtina teisės aktus, susijusius su Sistemos tvarkymu ir duomenų sauga;

6.3. priima sprendimą dėl Sistemos informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

6.4. kontroliuoja, kad Sistema būtų tvarkoma vadovaujantis Lietuvos Respublikos įstatymais, šiais Saugos nuostatais ir kitais teisės aktais;

6.5. atsako už tinkamą šiame punkte nustatytų funkcijų vykdymą.

7. Sistemos Tvarkytojo vadovo funkcijos ir atsakomybė:

7.1. Sistemos Valdytojo vadovo pavedimu skiria Sistemos saugos įgaliotinį;

7.2. skiria Sistemos administratorių arba kelis Sistemos administratorius, vykdančius atskiras Sistemos administravimo funkcijas (toliau - Administratorius);

7.3. atlieka Sistemos duomenų bazių ir tarnybinių stočių priežiūrą;

7.4. užtikrina Sistemos sąveiką su kitomis informacinėmis sistemomis ir registrais;

7.5. užtikrina nepertraukiamą Sistemos veikimą ir duomenų saugomų ir apdorojamų Sistema, saugą;

7.6. Sistemos Tvarkytojo ir Sistemos duomenų gavėjų sutartyse dėl duomenų teikimo nustatyta tvarka teikia Sistemos duomenis duomenų gavėjams;

7.7. atlieka kitas Sistemos nuostatų, Saugos nuostatų ir kitų teisės aktų nustatytas funkcijas;

7.8. teikia pasiūlymus Sistemos Valdytojui dėl duomenų saugos tobulinimo;

7.9. ne rečiau kaip kartą per metus, atlikus Sistemos rizikos analizę ir informacinių technologijų saugos atitikties vertinimą, esant poreikiui, organizuoja Sistemos saugos dokumentų atnaujinimą;

7.10. Sistemos Tvarkytojo vadovas yra atsakingas už tinkamą šiame punkte nustatytų funkcijų vykdymą.

8. Sistemos saugos įgaliotinis, įgyvendindamas Sistemos saugos priemones, atlieka šias funkcijas:

8.1. teikia Sistemos Tvarkytojo vadovui pasiūlymus dėl:

8.1.1. Sistemos Administratoriaus ar Administratorių paskyrimo;

8.1.2. Sistemos Saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

8.1.3. Sistemos informacinių technologijų saugos reikalavimų atitikties vertinimo organizavimo;

8.2. koordinuoja elektroninės informacijos saugos incidentų, įvykusių Sistemoje, tyrimą, išskyrus atvejus, kai šią funkciją atlieka informacijos saugos darbo grupės;

8.3. teikia Administratoriui privalomus vykdyti nurodymus ir pavedimus;

8.4. kasmet organizuoja:

8.4.1. Sistemos rizikos vertinimą;

8.4.2. Sistemos informacinių technologijų saugos reikalavimų atitikties vertinimą;

8.5. rengia Sistemos naudotojams seminarus informacijos saugos klausimais, informuoja juos apie informacijos saugos problematiką (siunčia priminimus elektroniniu paštu, rengia teminius seminarus, atmintines naujiems naudotojams);

8.6. atlieka kitas Sistemos Valdytojo vadovo ir Sistemos Tvarkytojo vadovų pavestas ir Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimo Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ jam priskirtas funkcijas.

9. Administratorius, vykdantis Sistemos priežiūrą, atlieka šias funkcijas:

9.1. vertina Sistemos naudotojų pasirengimą dirbti su Sistema;

9.2. rengia, tikrina ir analizuoja Sistemą sudarančių komponentų sąranką ir būsenos rodiklius;

9.3. pastebėjęs esamą arba tikėtiną Sistemos saugumo spragą, informuoja atsakingus asmenis;

9.4. informuoja Sistemos saugos įgaliotinį apie informacijos saugos pažeidimus, nusikalstamos veikos požymius, neveikiančias ar netinkamai veikiančias Sistemos duomenų saugos užtikrinimo priemones.

10. Saugų Sistemos duomenų tvarkymą reglamentuoja:

10.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

10.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

10.3. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

10.4. Lietuvos standartai LST ISO/IEC 27001:2006 ir LST ISO/IEC 27002:2009, Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo technika“ grupės standartai, nustatantys saugų informacinės sistemos duomenų tvarkymą;

10.5. Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtinti Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71;

10.6. kiti teisės aktai, reglamentuojantys elektroninės informacijos Saugos politiką ir duomenų tvarkymo teisėtumą, valstybės informacinių sistemų tvarkytojų veiklą ir duomenų saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

11. Sistema, vadovaujantis 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“, priskiriama prie ketvirtos kategorijos informacinių sistemų dėl joje apdorojamos vidaus informacijos svarbos ir kritiškumo, kurios praradimas neturėtų reikšmingos įtakos institucijų veiklai.

12. Elektroninės informacijos priskyrimas prie tam tikros kategorijos nustatomas įvertinus tvarkomų duomenų tipą ir poveikį Sistemos funkcionalumui atsižvelgiant į jų konfidencialumą, vientisumą ir pasiekiamumą.

13. Sistemos saugos įgaliotinis, vadovaudamasis Lietuvos standartu LST ISO/IEC 27005:2011 „Informacijos technologija. Saugumo technika. Informacijos saugumo rizikos valdymas“, kasmet organizuoja ir vykdo Sistemos rizikos veiksnių vertinimą. Prireikus, Sistemos saugos įgaliotinis gali organizuoti neeilinį Sistemos rizikos veiksnių vertinimą.

14. Sistemos rizikos veiksnių vertinimas surašomas Sistemos rizikos įvertinimo ataskaitoje. Sistemos rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti poveikį informacijos saugai. Svarbiausi rizikos veiksniai yra šie:

14.1. subjektyvūs netyčiniai (duomenų tvarkymo klaidos ir apsirikimai, dalinis duomenų ištrynimas, atsitiktinis klaidingų duomenų teikimas, fiziniai informacinių technologijų sutrikimai, duomenų perdavimo kompiuterių tinklais sutrikimai, programinės įrangos klaidos, netinkamas veikimas ir kita);

14.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis Sistemos duomenims gauti, Sistemos duomenų pakeitimas ar sunaikinimas, tyčiniai informacinių technologijų duomenų perdavimo kompiuterių tinklais sutrikdymai, piktybiniai Sistemos saugumo pažeidimai, vagystės ir kita);

14.3. nenugalima jėga (*force majeure*).

15. Rizikos veiksniai vertinami pagal elektroninės informacijos kategorijas, nustatant jų poveikio Sistemos elektroninės informacijos saugai laipsnius:

15.1. Ž – žemas. Duomenų pažeidimo poveikio laipsnis nėra didelis, padariniai nėra pavojingi – informacija nusiųsta kitam adresatui, įvesti netikslūs duomenys, dingo dalis informacijos, kurią galima greitai atkurti iš turimų atsarginių duomenų kopijų, prarasta informacija po paskutinio kopijavimo;

15.2. V – vidutinis. Duomenų pažeidimo poveikio laipsnis gali būti didelis, padariniai rimti – duomenys netikslūs ar sugadinti, bet juos įmanoma atkurti iš turimų atsarginių kopijų, duomenų bazių įrašai pakeisti, sunku rasti klaidas ir suklastotą informaciją, neveikia kompiuterių programos ir operacinė sistema;

15.3. A – aukštas. Duomenų pažeidimo poveikio laipsnis labai didelis, padariniai rimti – duomenys visiškai sugadinti, dėl vagystės, gaisro ar užliejimo prarasti ne tik duomenų bazių duomenys, bet ir atsarginės kopijos, neveikia visa Sistema.

16. Sistemos rizikos vertinimo darbų apimtis:

16.1. Sistemą sudarančių informacinių išteklių inventorizacija;

16.2. poveikio Sistemos veiklai vertinimas;

16.3. grėsmės ir pažeidimų analizė;

16.4. liekamosios rizikos vertinimas.

17. Sistemos Valdytojas, atsižvelgdamas į Sistemos rizikos įvertinimo ataskaitą, prireikus, tvirtina Sistemos rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis Sistemos rizikos valdymo priemonėms įgyvendinti.

18. Pagrindiniai elektroninės informacijos saugos priemonių parinkimo principai yra šie:

18.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

18.2. informacijos saugos priemonės diegimo kaina turi būti adekvati saugomos informacijos vertei;

18.3. kur galima, turi būti įdiegtos prevencinės, grėsmes aptinkančios ir jas mažinančios informacijos saugos priemonės.

19. Siekiant užtikrinti šiuose Saugos nuostatuose ir kituose Saugos politiką įgyvendinančiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, ne rečiau kaip kartą per metus yra organizuojamas informacinių technologijų saugos atitikties vertinimas, kurio metu:

19.1. vertinama šių Saugos nuostatų ir kitų Saugos politiką įgyvendinančių teisės aktų ir realios informacijos augos atitiktis;

19.2. inventorizuojama sistemos techninė ir programinė įranga;

19.3. tikrinama Sistemos tarnybinėse stotyse įdiegta programinė įranga ir jų sąranka;

19.4. tikrinama (vertinama) Sistemos duomenis tvarkantiems naudotojams ir Sistemos Administratoriui suteiktų teisių atitiktis jų vykdomoms funkcijoms;

19.5. vertinamas pasirengimas užtikrinti Sistemos veiklos tęstinumą įvykus saugos incidentui.

20. Atlikus šių Saugos nuostatų 19 punkte nurodytą vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato Sistemos Valdytojo vadovas.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

21. Priemonės ir metodai, taikomi užtikrinant prieigą prie Sistemos, nurodant leistiną šios prieigos laiką ir būdą, nustatomi Sistemos naudotojų administravimo taisyklėse.

22. Visos Sistemos tarnybinės stotys ir kompiuterizuotos darbo vietos turi būti apsaugotos nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto laiškų ir kitos kenksmingos programinės įrangos). Apsaugai naudojama programinė įranga turi būti centralizuotai valdoma ir atsinaujinti automatiškai ne rečiau kaip kartą per 24 valandas.

23. Naudoti programinę įrangą, nesusijusią su Sistemos Tvarkytojo veikla ir atliekamomis funkcijomis (žaidimų, bylų siuntimo, internetinių pokalbių programų ir kt.), draudžiama.

24. Sistemos naudotojų prieiga prie kitų valstybės institucijų arba žinybinių kompiuterių tinklų ar interneto turi būti apsaugota užkardomis. Interneto turinys turi būti kontroliuojamas, nepraleidžiant nepageidaujamos informacijos. Už kompiuterių tinklo filtravimo įrangos administravimą ir priežiūrą atsakingas Turto valdymo ir viešųjų pirkimų skyriaus vyresnysis specialistas, kurio veiklos sritis yra Valstybinės kainų ir energetikos kontrolės komisijos kompiuterinės techninės bazės priežiūra.

25. Sistemos vartotojams, savo tarnybinėms funkcijoms vykdyti naudojantiems nešiojamus kompiuterius Sistemos duomenų perdavimui kompiuterių tinklais ne savo darbo vietoje, šiuose kompiuteriuose turi būti naudojamas kompiuterio įjungimo slaptažodis, papildomas Sistemos vartotojo tapatybės patvirtinimas ir Sistemos duomenų šifravimas.

26. Sistemos atsarginių kopijų darymui skirta kompiuterinė ir programinė įranga. Pačių atsarginių kopijų ruošimo, atstatymo ir kokybės testavimas yra aprašomas Valstybinės kainų ir energetikos kontrolės komisijos rezervinių kopijų ruošimo vadove, patvirtintame Valstybinės kainų ir energetikos kontrolės komisijos pirmininko 2015 m. d. įsakymu Nr. .

27. Sistema nuo išorinių viešųjų kompiuterių tinklų turi būti atskirta naudojant įgaliotąją tarnybinę stotį. Įgaliotoje tarnybinėje stotyje turi būti fiksuojama ir Saugos politika įgyvendinančiuose dokumentuose nustatytą laiką saugoma informacija apie visų Sistemos naudotojų kreipinius.

28. Automatiniai duomenų mainai tarp informacinių sistemų turi būti vykdomi tik naudojant saugias ryšio linijas su perduodamų duomenų šifravimu. Duomenų šifravimo algoritmas – ne žemesnis nei 128 bitų raktą turintis AES (angl. „Advanced Encryption Standard“ – Pažangus šifravimo standartas).

29. Vartotojai jungdamiesi prie VKEKK Elektros kainų palyginimo sistemos iš nutolusių darbo vietų per viešuosius kompiuterių tinklus privalo naudoti tik saugias HTTPS jungtis.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

30. Sistemos naudotojai privalo rūpintis tvarkomos informacijos saugumu.

31. Visi Sistemos naudotojai privalo turėti darbo kompiuteriu įgūdžių, mokėti tvarkyti Sistemos duomenis Sistemos nuostatų nustatyta tvarka ir būti susipažinę su Sistemos Saugos nuostatais ir Saugos politikos įgyvendinimą reglamentuojančiais teisės aktais.

32. Sistemos saugos įgaliotinis privalo išmanyti informacijos saugos užtikrinimo principus, savo darbe vadovautis Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156, kitais teisės aktais. Sistemos saugos įgaliotinis privalo prižiūrėti, kaip įgyvendinama Saugos politika, taip pat turėti darbo su duomenų bazėmis, operacinėmis sistemomis, taikomosiomis programomis patirties, negali turėti neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

33. Sistemos Administratoriumi gali būti skiriamas valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, išmanantis darbą su kompiuterių tinklais ir gebantis administruoti tarnybines stotis bei mokantis užtikrinti jų saugumą. Sistemos Administratorius privalo mokėti administruoti duomenų bazes. Gali būti skiriami ir keli Sistemos Administratoriai.

34. Sistemos saugos įgaliotinis ne rečiau kaip kartą per dvejus metus inicijuoja Sistemos naudotojų mokymą informacijos saugos klausimais.

V SKYRIUS
ELEKTROS KAINŲ PALYGINIMO SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

35. Už Sistemos naudotojų supažindinimą su šiais Saugos nuostatais ir kitais Saugos politiką įgyvendinančiais teisės aktais yra atsakingas Sistemos saugos įgaliotinis.

36. Sistemos saugos įgaliotinis atsakingas už tai, kad šie Saugos nuostatai ir kiti Saugos politiką įgyvendinantys teisės aktai būtų paskelbti Sistemos naudotojams pasiekiamame tinklalapyje. Pakeitus arba paskelbus naujus dokumentus Sistemos naudotojai apie tai informuojami elektroniniu paštu.

37. Sistemos Administratorių su šiais Saugos nuostatais ir kitais Saugos politiką įgyvendinančiais teisės aktais bei atsakomybe už šių reikalavimų nesilaikymą supažindina Sistemos saugos įgaliotinis.

38. Pakartotinai su Saugos politiką reguliuojančiais teisės aktais Sistemos naudotojai supažindinami tik iš esmės pasikeitus informacinėms sistemoms arba informacijos saugą reguliuojantiems teisės aktams. Informacija apie Saugos politiką įgyvendinančių teisės aktų pasikeitimus skelbiama Sistemos vartotojams pasiekiamame tinklalapyje www.regula.lt.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

39. Sistemos naudotojai, Valdytojo vadovas, Tvarkytojo vadovas, saugos įgaliotinis bei Administratorius pažeidę saugos dokumentuose nustatytus reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

_____