

VALSTYBINĖS KAINŲ IR ENERGETIKOS KONTROLĖS KOMISIJOS ELEKTROS ENERGIJOS KAINŲ PALYGINIMO INFORMACINĖS SISTEMOS VEIKLOS TĖSTINUMO VALDYMO PLANAS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Valstybinės kainų ir energetikos kontrolės komisijos (toliau – Komisija) elektros energijos kainų palyginimo informacinės sistemos (toliau – Sistema) veiklos tęstinumo valdymo planas (toliau – Planas) reglamentuoja Sistemos ir jos teikiamų funkcijų nepertraukiamos veiklos užtikrinimą.

2. Planas parengtas 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 aktyviają 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 vidinis administratorius** – Komisijos įsakymu paskirtas valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį, sistemoje turintis aukščiausio lygio teises, vykdamas Sistemos išorinių naudotojų teisių ir duomenų tvarkymo priežiūrą;

3.4. **Sistemos išorinis naudotojas** – Ūkio subjektas (Ūkio subjekto atstovas), kuris naudojami Sistema duomenų teikimui ir kitiems susijusiems veiksams atlikti;

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

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

3.6. **Elektroninės informacijos saugos incidentas** – įvykis ar veiksmas, kuris gali sudaryti neteisėto prisijungimo prie Sistemos galimybę, sutrikdyti ar pakeisti Sistemos veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti.

4. Kitos Plane vartojamos 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. Saugos įgaliotinis yra atsakingas už Plano ir susijusių dokumentų rengimo organizavimą.

6. Plano įgyvendinimui nustatomos funkcijos ir įgaliojimai:

6.1. Saugos įgaliotinis dalyvauja Sistemos veiklos tęstinumą užtikrinančioje veiklos tęstinumo valdymo grupėje (toliau – Valdymo grupė) ir teikia jai informaciją apie elektroninės informacijos saugos incidentus;

6.2. Sistemos administratorius užtikrina sistemų atkūrimą;

6.3. Sistemos naudotojai privalo vykdyti Plano Valdymo grupės reikalavimus.

7. Planas įsigalioja, įvykus elektroninės informacijos saugos incidentui, esant didelei jo tikimybei arba Valdymo grupės vadovo sprendimu.

8. Finansinių ir kitokių išteklių, numatomų Sistemos veiklai atkurti, paskelbus elektroninės informacijos saugos incidentą, šaltinius ir, pobūdį numato ir pasirenka Valdymo grupė.

9. Sistemos prieinamumas turi būti ne mažiau kaip 90 proc. laiko visą parą.

10. Maksimali Sistemos veiklos sutrikimo trukmė – 16 val.

11. Sistemos veikla yra laikoma atkurta tuomet, kai Sistemos naudotojai vėl gali atlikti savo darbine funkcijas įprastiniu būdu.

12. Saugos įgaliotinis informaciją apie saugos incidentą įrašo į Sistemos elektroninės informacijos saugos incidentų registravimo žurnalą (2 priedas), vykdo Valdymo bei Atkūrimo grupės pavestas funkcijas, atlieka Sistemos veiklos atkūrimo detalajame plane (1 priedas) numatytus veiksmus.

II SKYRIUS

VEIKLOS VALDYMO IR ATKŪRIMO PRINCIPAI

13. Pagrindiniai elektroninės informacijos saugos incidentų valdymo principai prioriteto tvarka yra šie:

13.1. Komisijos valstybės tarnautojų ar darbuotojų, dirbančių pagal darbo sutartį, (toliau – Darbuotojai) gyvybės ir sveikatos apsaugos užtikrinimas. Būtina užtikrinti visų Darbuotojų gyvybės ir sveikatos apsaugą, kol trunka elektroninės informacijos saugos incidentas ir likviduojami jo padariniai;

13.2. Sistemos veiklos atkūrimas. Paskelbus elektroninės informacijos saugos incidentą, jei būtina, organizuojama Sistemos fizinė sauga ir jos veiklos atkūrimas. Visų pirma yra atkuriamos kritiškiausios Sistemos funkcijos ir užtikrintas jų prieinamumas;

13.3. Plano arba jo dalių veiksmingumo išbandymas. Plano arba jo dalių veiksmingumas yra reguliariai išbandomas Veiklos tęstinumo valdymo grupės iniciatyva ir, jei būtina, koreguojamas, atsižvelgiant į rastus trūkumus;

13.4. Darbuotojų mokymas. Darbuotojai yra supažindinami su Planu ir kitais teisės aktais, nustatančiais asmeninę kiekvieno Darbuotojo atsakomybę, kai įvyksta elektroninės informacijos saugos incidentas.

14. Pagrindiniai Sistemos, ryšių ir infrastruktūros atkūrimo principai yra šie:

14.1. Sistemos veikimui būtinos infrastruktūros atkūrimo pirmumas. Pirmiausia būtina atkurti kritiškiausias Sistemos funkcijas;

14.2. pakankamo Sistemos sudarančios techninės įrangos, ryšių ir infrastruktūros rezervo užtikrinimas. Rezervuota minimaliai būtina įranga, reikalinga kritinėms Sistemos funkcijoms vykdyti;

14.3. už Sistemos komponentų, ryšių ir infrastruktūros atkūrimą atsakingų Darbuotojų mokymai. Mokymai ir Plano bandymai organizuojami reguliariai. Jei Planas pakeičiamas, atsakingi Darbuotojai nedelsiant supažindinami su pakeitimais.

III SKYRIUS ORGANIZACINĖS NUOSTATOS

15. Sistemos veiklos tęstinumą koordinuoja Valdymo grupė.
16. Valdymo grupę sudaro:
 - 16.1. Valdymo grupės vadovas – Komisijos Administracijos direktorius;
 - 16.2. Valdymo grupės vadovo pavaduotojas – Komisijos Dujų ir elektros departamento Elektros skyriaus vedėjas;
 - 16.3. Valdymo grupės vadovo pavaduotojas – Komisijos Veiklos valdymo skyriaus vedėjas;
 - 16.4. Sistemos administratorius – Turto valdymo ir viešųjų pirkimų skyriaus vyresn. specialistas ir Sistemos priežiūros ir palaikymo paslaugas teikiantis tiekėjas;
 - 16.5. Sistemos saugos įgaliotinis – Turto valdymo ir viešųjų pirkimų skyriaus vyr. specialistas;
 - 16.6. Valdymo grupės narys – Komisijos Turto valdymo ir viešųjų pirkimų skyriaus specialistas atsakingas už darbų ir priešgaisrinę saugą.
17. Koordinuodama Sistemos veiklos tęstinumą, Valdymo grupė atlieka šias veiklas:
 - 17.1. analizuoja situaciją ir priima sprendimus dėl Sistemos veiklos tęstinumo;
 - 17.2. bendrauja su darbuotojais, tiekėjais, teisėsauga ir kitomis institucijomis;
 - 17.3. prižiūri finansinių ir kitų išteklių, reikalingų Sistemos veiklai atkurti, įvykus elektroninės informacijos saugos incidentui, naudojimą;
 - 17.4. koordinuoja elektroninės informacijos fizinę saugą elektroninės informacijos saugos incidento metu;
 - 17.5. koordinuoja Darbuotojų ir įrangos gabenimą;
 - 17.6. vykdo Sistemos veiklos atkūrimo priežiūrą ir koordinavimą.
18. Sistemos veiklą atkuria veiklos atkūrimo grupė (toliau – Atkūrimo grupė).
19. Atkūrimo grupę sudaro:
 - 19.1. Atkūrimo grupės vadovas – Komisijos Turto valdymo ir viešųjų pirkimų skyriaus vedėjas;
 - 19.2. Atkūrimo grupės vadovo pavaduotojas – Komisijos Turto valdymo ir viešųjų pirkimų skyriaus vedėjo pavaduotojas;
 - 19.3. Atkūrimo grupės nariai – Komisijos Dujų ir elektros departamento Elektros skyriaus specialistai (ne mažiau 2 darbuotojų);
 - 19.4. Atkūrimo grupės nariai – Turto valdymo ir viešųjų pirkimų skyriaus IT specialistai, Sistemos priežiūros ir palaikymo paslaugas teikiantis tiekėjas (ne mažiau 2 darbuotojų).
20. Atkūrimo grupės funkcijos:
 - 20.1. tarnybinių stočių veikimo atkūrimas;
 - 20.2. vidaus duomenų perdavimo tinklo veikimo atkūrimas;
 - 20.3. Sistemos duomenų atkūrimas;
 - 20.4. taikomųjų programų tinkamo veikimo atkūrimas;
 - 20.5. Sistemos naudotojų kompiuterių veikimo atkūrimas ir prijungimas prie vidaus duomenų perdavimo tinklo.
21. Įvykus elektroninės informacijos saugos incidentui, Atkūrimo grupė kas 2 val. turi informuoti Valdymo grupės vadovą apie Sistemos atkūrimo eigą.
22. Valdymo ir Atkūrimo grupės tarpusavyje komunikuoja tiesiogiai, telefonu ar elektroniniu paštu.

23. Sistemos veiklos atkūrimo detalų planą parengia Sistemos administratorius ir Sistemos vidinis administratorius. Saugos įgaliotinis įvertina parengtus planus ir informuoja Turto valdymo ir viešųjų pirkimų skyriaus vedėją.

24. Numatytose atsarginėse patalpose, naudojamose Sistemos veiklai atkurti, elektroninės informacijos saugos incidento atveju, yra:

24.1. parengta ir veikianti duomenų perdavimo tinklo prieiga;

24.2. tiekiamas nepertraukiamas elektros maitinimas tarnybinėms stotims ir duomenų perdavimo tinklo įrangai;

24.3. įdiegtos įrangos kondicionavimo sistemos, užtikrinančios reikiamą patalpų temperatūrą ir drėgnumą;

24.4. rakinamos durys.

25. Valdymo ir Atkūrimo grupių nariai turi reaguoti ir valdyti elektroninės informacijos saugos incidentus, vadovaudamiesi 1 priede nurodytais veiksmais.

26. Sistemos naudotojai turi reaguoti į elektroninės informacijos saugos incidentus, vadovaudamiesi 1 priede nurodytais veiksmais.

IV SKYRIUS APRAŠOMOSIOS NUOSTATOS

27. Parengtų ir Komisijoje saugomų dokumentų sąrašas:

27.1. Sistemos specifikacijos kopija, kurioje nurodyti Sistemos techninės ir programinės įrangos parametrai. Specifikacijos projektą rengė Viešųjų pirkimų įstatymo nustatyta tvarka parinktas paslaugų teikėjas. Už Sistemos techninės ir programinės įrangos priežiūrą atsakingas Sistemos administratorius, kuriam keliami kvalifikaciniai reikalavimai, nurodyti Sistemos duomenų saugos nuostatuose, patvirtintuose 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“. Nesant administratoriaus, kuris dėl komandiruotės, ligos ar kitų priežasčių negali operatyviai atvykti į darbo vietą, jį pavaduoti gali kitas Komisijos pirmininko paskirtas darbuotojas, kurio kompetencijos lygis informacinių technologijų srityje atitinka Sistemos administratoriui keliamų reikalavimų lygį arba įmonė su kuria pagal numatytus atlikti darbus ir įkainius pasirašyta priežiūros ir palaikymo paslaugų sutartis;

27.2. Komisija naudoja (pagal nuomos, panaudos ar kitas sutartis) visą Sistemos techninę įrangą, priklausančią ir esančią trečiosios šalies patalpose – sutarties su trečiaja šalimi data ir numeris; sutarties kopija saugoma pas Atkūrimo grupės vadovą.

27.3. Komisijos patalpų, kuriose yra komutacinė įranga, patalpų planai, kompiuterinio tinklo, kompiuterinių darbo vietų išdėstymo ir loginio sujungimo schemos. Už šių dokumentų rengimą atsakingas Atkūrimo grupės narys (Turto valdymo ir viešųjų pirkimų skyriaus IT specialistas);

27.4. Sistemos elektroninės informacijos teikimo, programinės įrangos priežiūros sutarčių kopijos, už kurių rengimą atsakingas Sistemos saugos įgaliotinis;

27.5. Sistemos techninės ir programinės įrangos sąrašai, kuriuose nurodyta programinės įrangos laikmenų ir laikmenų su atsarginėmis kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos. Už Sistemos techninės ir programinės įrangos sąrašų rengimą atsakingas Sistemos administratorius;

27.6. Sistemos duomenų rezervinių kopijų kūrimo instrukcija, kurioje nurodyta laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos. Už Sistemos duomenų rezervinių kopijų kūrimo instrukcijos parengimą atsakingas Sistemos saugos įgaliotinis;

27.7. Valdymo grupės ir Atkūrimo grupės narių sąrašas su kontaktiniais duomenimis, leidžiančiais pasiekti šiuos asmenis bet kuriuo metu. Už šių dokumentų parengimą atsakingas Atkūrimo grupės vadovo pavaduotojas.

28. Valdymo plano 27 punkte nurodytų dokumentų kopijas saugo Valdymo grupės vadovas.

V SKYRIUS PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

28. Plano veiksmingumo išbandymą organizuoja Saugos įgaliotinis.
29. Plano veiksmingumas išbandomas ne rečiau kaip kartą per metus.
30. Prieš įdiegiant naujus Sistemos komponentus, pradedant teikti naujas paslaugas arba pasikeitus veiklos aplinkai, Saugos įgaliotinis peržiūri Planą ir, esant reikalui, atlieka neeilinį Plano veiksmingumo išbandymą.
31. Plano veiksmingumas išbandomas simuliacinio būdu pagal elektroninės informacijos saugos incidento scenarijų.
32. Plano veiksmingumo išbandyme dalyvauja visi Valdymo grupės nariai. Esant reikalui, į plano veiksmingumo išbandymą gali būti pakviesti kiti Darbuotojai, tiekėjų arba kitų organizacijų atstovai.
33. Išbandžius Plano veiksmingumą, Saugos įgaliotinis parengia Plano veiksmingumo išbandymo ataskaitą ir pateikia ją Valdymo grupei. Plano veiksmingumo išbandymo ataskaitos šablonas yra pateiktas 3 priede.
34. Atsižvelgdamas į Plano veiksmingumo išbandymo metu pastebėtus trūkumus, Saugos įgaliotinis Valdymo grupei pateikia siūlymus dėl Plano pakeitimų arba papildymų.
35. Plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami, vadovaujantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

VI SKYRIUS BAIGIAMOSIOS NUOSTATOS

36. Plane numatyti veiksmai yra privalomi Sistemos valdytojui, Sistemos naudotojams, Sistemos administratoriui bei Saugos įgaliotiniui.
 37. Saugos įgaliotinis privalo supažindinti Sistemos naudotojus su Plano 1 priedu.
 38. Plane numatytų veiksmų laikymosi priežiūrą organizuoja Saugos įgaliotinis.
-

Valstybinės kainų ir energetikos kontrolės komisijos duomenų surinkimo ir analizės informacinės sistemos veiklos tęstinumo valdymo plano 1 priedas

VALSTYBINĖS KAINŲ IR ENERGETIKOS KONTROLĖS KOMISIJOS ELEKTROS ENERGIJOS KAINŲ PALYGINIMO INFORMACINĖS SISTEMOS VEIKLOS ATKŪRIMO DETALUSIS PLANAS

Elektroninės informacijos incidentas	Pirmaeiliai veiksmai	Veiklos atkūrimo veiksmai	Veiklos atkūrimo veiksmų vykdytojai
1. Pavojingų gamtinių reiškinių sukeltas incidentas	1.1. Elektroninės informacijos Saugos incidento pasekmės įvertinimas, priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas ir įgyvendinimas	1.1.1. Elektroninės informacijos saugos incidento metu padarytos žalos įvertinimas	Valdymo grupė
		1.1.2. Pavojaus sustabdymo ir padarytos žalos likvidavimo priemonių plano sudarymas ir paskelbimas	Valdymo grupės vadovo pavaduotojas Saugos įgaliotinis Sistemos administratorius
		1.1.3. Priemonių plano įgyvendinimas	Valdymo grupės vadovo pavaduotojas Saugos įgaliotinis Sistemos administratorius Valdymo grupės narys
	1.2. Darbuotojų elektroninės informacijos saugos incidento pasekmei likviduoti paskyrimas	1.2.1. Žalą likviduojančių darbuotojų instruktavimas	Saugos įgaliotinis Valdymo grupės narys
		1.2.2. Žalą likviduojančių darbuotojų veiksmų koordinavimas	Saugos įgaliotinis Valdymo grupės narys
	1.3. Oro prognozės sekimas	1.3.1. Žalą likviduojančių darbuotojų instruktavimas	Saugos įgaliotinis Valdymo grupės narys
	1.4. Dirbantiems pavojaus vietoje rekomendacijų teikimas	1.4.1. Elektroninės informacijos saugos incidento pasekmes likviduojančių darbuotojų instruktavimas	Saugos įgaliotinis Sistemos administratorius
		1.4.2. Darbuotojų informavimas apie elgseną pavojaus vietoje	Saugos įgaliotinis Valdymo grupės narys

Elektroninės informacijos incidentas	Pirmaeiliai veiksmai	Veiklos atkūrimo veiksmai	Veiklos atkūrimo veiksmų vykdytojai
		1.4.3. Pirmosios pagalbos suteikimo organizavimas nukentėjusiems darbuotojams	Saugos įgaliotinis Valdymo grupės narys
		1.4.4. Nukentėjusių darbuotojų gabenimo į gydymo įstaigą organizavimas	Valdymo grupės vadovo pavaduotojas Saugos įgaliotinis Valdymo grupės narys
	1.5. Pavojaus vietų ženklavimas	1.5.1. Darbuotojų informavimas	Valdymo grupės vadovo pavaduotojas Saugos įgaliotinis Valdymo grupės narys
		1.5.2. Žalą likviduojančių darbuotojų instruktavimas	Valdymo grupės vadovo pavaduotojas Saugos įgaliotinis Valdymo grupės narys
2. Gaisro sukeltas incidentas	2.1. Ugniagesių tarnybos informavimas	2.1.1. Įvykio vietos lokalizavimas, jei yra rekomendacija	Valdymo grupė
		2.1.2. Galimybių evakuoti darbuotojus paieška, jei yra rekomenduojama tai padaryti	Valdymo grupės vadovo pavaduotojas Saugos įgaliotinis Valdymo grupės narys
	2.2. Darbuotojų evakavimas (pagal ugniagesių tarnybos rekomendaciją)	2.2.1. Darbuotojų informavimas apie evakavimą, jei yra rekomendacija	Valdymo grupės vadovo pavaduotojas Saugos įgaliotinis Valdymo grupės narys
	2.3. Darbas pavojaus zonoje	2.3.1 Darbuotojų informavimas apie saugų darbą pavojaus zonoje	Valdymo grupės vadovo pavaduotojas Saugos įgaliotinis Valdymo grupės narys

Elektroninės informacijos incidentas	Pirmaeiliai veiksmai	Veiklos atkūrimo veiksmai	Veiklos atkūrimo veiksmų vykdytojai
	2.4. Komunikacijų, sukeliančių pavojų, išjungimas. Gaisro gesinimas ankstyvoje stadijoje, jei yra rekomendacija dirbti pavojaus zonoje	2.4.1 Teisėsaugos tarnybos nurodymų vykdymas	Valdymo grupės vadovo pavaduotojas Saugos įgaliotinis Valdymo grupės narys
3. Patalpų užgrobimo sukeltas incidentas	3.1. Teisėsaugos tarnybos informavimas	3.1.1. Įvykio vietos lokalizavimas, jei yra teisėsaugos tarnybos rekomendacijos	Valdymo grupė
		3.1.2. Galimybių evakuoti darbuotojus nagrinėjimas, jei yra rekomendacija	Valdymo grupės vadovo pavaduotojas Saugos įgaliotinis Valdymo grupės narys
	3.2. Darbuotojų evakavimas, jei yra rekomendacija	3.2.1. Darbuotojų informavimas apie evakavimą	Valdymo grupės vadovo pavaduotojas Saugos įgaliotinis Valdymo grupės narys
	3.3. Patalpų užrakinimas, jei yra galimybė	3.3.1. Teisėsaugos tarnybos nurodymų vykdymas	Valdymo grupės vadovo pavaduotojas Saugos įgaliotinis Valdymo grupės narys
	3.4. Teisėsaugos tarnybos nurodymų vykdymas, jei yra rekomendacijų	3.4.1. Darbuotojų informavimas apie nurodymų vykdymą	Valdymo grupės vadovo pavaduotojas Saugos įgaliotinis Valdymo grupės narys
	3.5. Veiksmai išlaisvinus užgrotas patalpas	3.5.1. Padarytos žalos įvertinimas	Valdymo grupė,
3.5.2. Padarytos žalos likvidavimo priemonių plano sudarymas, paskelbimas, vykdymas		Atkūrimo grupė	
3.5.3. Žalą likviduojančių darbuotojų instruktavimas		Saugos įgaliotinis Valdymo grupės narys	
4. Patalpos pažeidimo arba praradimo sukeltas incidentas	4.1. Atitinkamos tarnybos informavimas apie pavojaus pobūdį	4.1.1. Suinteresuotos tarnybos rekomendacijų dėl galimybės dirbti pavojaus zonoje gavimas	Sistemos Saugos įgaliotinis
		4.1.2. Darbuotojų informavimas apie rekomendacijas	Saugos įgaliotinis

Elektroninės informacijos incidentas	Pirmaeiliai veiksmai	Veiklos atkūrimo veiksmai	Veiklos atkūrimo veiksmų vykdytojai
5. Energijos tiekimo sutrikimo sukeltas incidentas	5.1. Energijos tiekimo sutrikimo priežasčių nustatymas. Tarnybinės stoties, kitos techninės įrangos energijos maitinimo išjungimas 5.2. Kreipimasis į energijos tiekimo tarnybą dėl pavojaus trukmės ir sutrikimo pašalinimo galimybių 5.3. Sutrikimų pašalinimas	5.1.1. Sutrikimų šalinimo organizavimas 5.2.1. Rekomendacijų iš energijos tiekimo tarnybos gavimas 5.3.1. Pavojaus sustabdymas, padarytos žalos likvidavimo priemonių plano sudarymas ir įgyvendinimas 5.3.2. Padarytos žalos įvertinimas 5.4.3. Žalą likviduojančių darbuotojų instruktavimas	Atkūrimo grupė Valdymo grupė, Atkūrimo grupė Valdymo grupės vadovo pavaduotojas Saugos įgaliotinis Valdymo grupės narys Valdymo grupė Saugos įgaliotinis Valdymo grupės narys
6. Vandentiekio ir šildymo sistemos sutrikimų sukeltas incidentas	6.1. Vandentiekio ar šildymo paslaugų teikėjų informavimas 6.2. Sutrikimo šalinimo prognozės skelbimas, sutrikimo pašalinimas	6.1.1. Atitinkamos tarnybos paklausimas dėl leidimo dirbti ir rekomendacijų gavimas 6.1.2. Darbuotojų informavimas apie rekomendacijas 6.2.1. Padarytos žalos įvertinimas. Sutrikimo sustabdymo ir padarytos žalos likvidavimo priemonių plano sudarymas, plano įgyvendinimas 6.2.2. Žalą likviduojančių darbuotojų instruktavimas	Saugos įgaliotinis Valdymo grupės narys Saugos įgaliotinis Valdymo grupės narys Valdymo grupė, Atkūrimo grupė Saugos įgaliotinis Valdymo grupės narys
7. Ryšio sutrikimai ir panašiai	7.1. Ryšio sutrikimo priežasčių nustatymas 7.2. Ryšio tarnybų informavimas, paklausimo dėl sutrikimo trukmės ir pašalinimo prognozės	7.1.1. Kreipimasis į ryšio paslaugos teikėją 7.2.1. Nustatymas ir įgyvendinimas priemonių, kad sutrikimai nesikartotų	Sistemos Saugos įgaliotinis Valdymo grupės narys Saugos įgaliotinis Valdymo grupės narys

Elektroninės informacijos incidentas	Pirmaeiliai veiksmai	Veiklos atkūrimo veiksmai	Veiklos atkūrimo veiksmų vykdytojai
	7.3. Sutrikimo pašalinimas	7.3.1. Kreipimasis į kitą ryšio paslaugos teikėją, jei sutrikimas nepašalintas	Saugos įgaliotinis Valdymo grupės narys
8. Tarnybinės stoties, komutacinės įrangos sugadinimas	8.1. Pranešti teisėsaugos tarnybai, draudimo bendrovei apie įvykį	8.1. Darbuotojų elektroninės informacijos saugos incidento pasekmei likviduoti paskyrimas, instruktavimas, jų veiksmų nustatymas	Saugos įgaliotinis
	8.2. Elektroninės informacijos saugos incidento pasekmių šalinimas	8.2.1. Kreipimasis į įrangos tiekėjus dėl įrangos remonto ar naujos įsigijimo	Sistemos administratorius Saugos įgaliotinis
		8.2.2. Įsigytos įrangos diegimas	Sistemos administratorius Saugos įgaliotinis
9. Programinės įrangos sugadinimas, praradimas	9.1. Elektroninės informacijos saugos incidento pasekmės įvertinimas, priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas	9.1.1. Elektroninės informacijos saugos incidento metu padarytos žalos įvertinimas	Valdymo grupė, Atkūrimo grupė
		9.1.2. Priemonių plano sudarymas, paskelbimas ir įgyvendinimas	
	9.2. Darbuotojų elektroninės informacijos saugos incidento pasekmei likviduoti paskyrimas. Žalą likviduojančių darbuotojų instruktavimas, jų veiksmų koordinavimas	9.2.1. Žalą likviduojančių darbuotojų instruktavimas	Saugos įgaliotinis Valdymo grupės narys
		9.2.2. Kreipimasis į teisėsaugos tarnybas dėl programinės įrangos sugadinimo ar praradimo ir jų nurodymų vykdymas	Sistemos administratorius Saugos įgaliotinis
9.3. Programinės įrangos kopijų periodinis gaminimas	9.3.1 Sugadintos ar prarastos programinės įrangos atkūrimo organizavimas		
10. Dokumentų praradimas	10.1. Elektroninės informacijos saugos incidento pasekmių įvertinimas	10.1. Prarastų dokumentų atkūrimas	Valdymo grupė
		10.2. Prarastų dokumentų atkūrimo kontrolė	Valdymo grupė
11. Darbuotojų praradimas	11.1. Elektroninės informacijos saugos incidento pasekmių įvertinimas	11.1.1. Trūkstamų darbuotojų paieška ir priėmimas į darbą	Veiklos valdymo skyrius

Valstybinės kainų ir energetikos kontrolės komisijos
duomenų surinkimo ir analizės informacinės
sistemos veiklos tęstinumo valdymo plano
2 priedas

(Elektroninės informacijos saugos incidentų registravimo žurnalo formos pavyzdys)

SISTEMOS ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTŲ REGISTRAVIMO ŽURNALAS

Pildymo pradžia 20__m. _____ d.

Eil. Nr.	Elektroninės informacijos saugos incidentas						
	Registro tvarkytojo pavadinimas	Požymio kodas	Įvykio aprašymas	Pradžia (metai, mėnuo, diena, valanda)	Pabaiga (metai, mėnuo, diena, valanda)	Pašalino (vardas, pavardė)	Saugos įgaliotinis (vardas, pavardė, parašas)
1.							
2.							
3.							
4.							
5.							
6.							

Elektroninės informacijos saugos incidento požymiai:

1. oro sąlygos; 2. gaisras; 3. patalpų užgrobimas; 4. patalpai padaryta žala arba patalpos praradimas; 5. energijos tiekimo sutrikimai; 6. vandentiekio ir šildymo sistemos sutrikimai; 7. ryšio sutrikimai; 8. tarnybinės stoties, komutacinės įrangos sugadinimas, praradimas; 9. programinės įrangos sugadinimas, praradimas; 10. duomenų pakeitimas, sunaikinimas, atskleidimas, dokumentų praradimas; 11. darbuotojų praradimas.

Valstybinės kainų ir energetikos
kontrolės komisijos duomenų surinkimo
ir analizės informacinės sistemos veiklos
tęstinumo valdymo plano
3 priedas

**VEIKLOS TĘSTINUMO VALDYMO PLANO
VEIKSMINGUMO IŠBANDYMO ATASKAITA**

(Veiklos tęstinumo valdymo grupės susitikimo data ir dokumento numeris)

Išbandymo dalyvių sąrašas:

1. _____
2. _____
3. _____
- ... _____

Elektroninės informacijos saugos incidento scenarijaus apibūdinimas:

Sistemos komponentai, kuriuos paveikė elektroninės informacijos saugos incidentas:

Elektroninės informacijos saugos incidento valdymo eiga:

Rasti Plano trūkumai:

Pasiūlymai keisti arba papildyti Planą:

(vardas, pavardė)

(parašas)

(vardas, pavardė)

(parašas)

(vardas, pavardė)

(parašas)