PATVIRTINTA
Valstybinės kainų ir energetikos kontrolės komisijos pirmininko
2017 m. spalio 31 d. įsakymu Nr. O1E-109

VALSTYBINĖS KAINŲ IR ENERGETIKOS KONTROLĖS KOMISIJOS INFORMACIJOS SAUGUMO VALDYMO SISTEMOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės kainų ir energetikos kontrolės komisijos (toliau – Komisija) informacijos saugumo valdymo sistemos aprašas (toliau – Aprašas) reglamentuoja Komisijos informacijos saugumo valdymo sistemos (toliau – ISVS) įdiegimo reikalavimus.

2. Apraše naudojamos šios sąvokos ir trumpiniai:

2.1. **informacijos saugumas** – informacijos konfidencialumo, vientisumo ir pasiekiamumo išsaugojimas;

2.2. **ISVS** – informacijos saugumo valdymo sistema;

2.3. **rizika** – informacijos saugumo įvykio tikimybės ir jo padarinių derinys;

2.4. **rizikos valdymas** – darnūs veiksmai, kuriais, atsižvelgiant į riziką, siekiama koordinuoti ir kontroliuoti Komisijos veiklos riziką;

2.5. **informacijos saugos įgaliotinis** – Komisijos pirmininko įsakymu paskirtas Komisijos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį;

2.6. **vadovybė** – Komisijos pirmininkas, Komisijos nariai, Komisijos administracijos direktorius;

2.7. **vadovybės vertinamoji ISVS analizė** – tai vadovybės atliekamas visapusiškas veiklos nagrinėjimas, nustatantis ISVS efektyvumą, atitiktį reikalavimams bei numatantis galimus ISVS tobulinimo veiksmus.

II SKYRIUS
KOMISIJOS KONTEKSTAS

3. Komisija yra įstaiga, reguliuojanti energetikos, geriamojo vandens tiekimo ir nuotekų tvarkymo paslaugų teikimo srityse veikiančių subjektų veiklą ir atliekanti valstybinę energetikos priežiūrą.

4. Komisijos veiklos tikslai – pagal kompetenciją atlikti veiklos šilumos, gamtinių dujų, centralizuotai tiekiamų suskystintų naftos dujų, elektros, atsinaujinančių išteklių energetikos ir geriamojo vandens tiekimo ir nuotekų tvarkymo sektoriuose valstybinio reguliavimo funkcijas, užtikrinti reguliuojamosios šilumos, gamtinių dujų, centralizuotai tiekiamų suskystintų naftos dujų, elektros, atsinaujinančių išteklių energetikos ir geriamojo vandens tiekimo ir nuotekų tvarkymo veiklos vykdymo ir energetikos bei geriamojo vandens tiekimo ir nuotekų tvarkymo įmonių ir vartotojų teisių ir pareigų tinkamo įgyvendinimo priežiūrą ir kontrolę, sąžiningos konkurencijos laisvę energetikos, geriamojo vandens ir nuotekų tvarkymo sektoriuose.

5. ISVS suinteresuotos šalys yra:

5.1. Komisijos valstybės tarnautojai, pareigūnai ir darbuotojai, dirbantys pagal darbo sutartis (toliau – Darbuotojai);

5.2. reguliuojamos energetikos įmonės;

5.3. energetinių paslaugų vartotojai;

5.4. Energetikos reguliavimo institucijų bendradarbiavimo agentūra (angl. ACER, toliau – Agentūra);

5.5. Tiekėjai, teikiantys Komisijos informacinių sistemų kūrimo, modernizavimo ir priežiūros paslaugas;

5.6. kiti Tiekėjai, kurie turi prieigą prie Komisijos informacinių išteklių.

6. Komisijos informacinėse sistemose tvarkomi asmens duomenys, todėl Komisija siekia užtikrinti ne tik atitiktį asmens duomenų apsaugą reglamentuojantiems teisės aktams, bet ir garantuoti visoms suinteresuotoms šalims tinkamą informacijos saugumo lygį.

7. Taikytini informacijos saugumo išorės reikalavimai:

7.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

7.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

7.3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

7.4. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“;

7.5. Bendrųjų elektroninės informacijos saugos reikalavimų, Saugos dokumentų turinio gairių ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašai, patvirtinti 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“;

7.6. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti 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“;

7.7. Bendrieji reikalavimai organizacinėms ir techninėms asmens duomenų saugumo priemonėms, patvirtinti Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms asmens duomenų saugumo priemonėms patvirtinimo“;

7.8. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB;

7.9. 2011 m. spalio 25 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1227/2011 dėl didmeninės energijos rinkos vientisumo ir skaidrumo (toliau – REMIT);

7.10. REMIT informacijos saugumo politika.

8. Komisijos antros ir ketvirtos kategorijos informacinės sistemos naudojamos duomenų surinkimui ir analizei, todėl Komisija siekia užtikrinti šių sistemų nepertraukiamą veikimą (pasiekiamumą) ir informacijos tikslumą (vientisumą).

III SKYRIUS
KOMISIJOS INFORMACIJOS SAUGUMO VALDYMO SISTEMOS TAIKYMO SRITIS

9. ISVS taikymo sritis – energetikos, geriamojo vandens tiekimo ir nuotekų tvarkymo paslaugų teikimo srityse veikiančių subjektų veiklos reguliavimas ir valstybinė energetikos priežiūra.

10. ISVS taikoma visai Komisijoje naudojamai informacijai (nepriklausomai nuo jos formato ir saugojimo būdo), visiems procesams, visiems Darbuotojams, fiziniams ir juridiniams asmenims, kuriems teisės aktų ar sutartinių santykių pagrindu yra suteikta prieiga prie Komisijos informacijos ar informacijos apdorojimo priemonių, taip pat jų teikiamoms paslaugoms.

11. Komisija parengia, įformina dokumentais, prižiūri ir nuolat tobulina ISVS, siekdama valdyti Komisijos veiklai kylančias informacijos saugumo rizikas.

12. ISVS reglamentuojančių dokumentų sąrašas pateiktas Aprašo 20 punkte.

13. Informacijos saugos įgaliotinis yra atsakingas už ISVS veiklų koordinavimą ir užtikrina, kad apie susijusius su ISVS sprendimus būtų informuoti visi su šiais sprendimais susiję Komisijos darbuotojai.

14. Darbuotojai privalo būti susipažinę su informacijos saugą reglamentuojančiais teisės aktais.

IV SKYRIUS
KOMISIJOS VADOVYBĖ

15. Vadovybė įsipareigoja užtikrinti ISVS įgyvendinimą, nuolatinę ISVS plėtrą bei gerinimą. Vadovybės funkcijos:

15.1. nustatyti ISVS politiką;

15.2. nustatyti ISVS tikslus bei patvirtinti ISVS planus;

15.3. numatyti su informacijos saugumu susijusias pareigas ir atsakomybes;

15.4. sudaryti sąlygas Komisijos darbuotojams tobulinti žinias informacijos saugumo srityje bei informuoti Komisijos darbuotojus apie atsakomybę už informacijos saugumo pažeidimus;

15.5. užtikrinti efektyvų ISVS aprūpinimą reikiamais ištekliais: žmogiškaisiais ištekliais, infrastruktūra (patalpos, programinė įranga, ryšiai ir kt.), nustatyti, kurios paslaugos yra perkamos, tinkamomis darbo sąlygomis;

15.6. numatyti rizikos prisiėmimo ir priimtinų rizikos lygių kriterijus;

15.7. užtikrinti reguliarius ISVS vidaus auditus;

15.8. atlikti vadovybės vertinamąją ISVS analizę.

16. Vadovybė nustato Komisijos darbuotojams būtiną turėti kvalifikaciją, kuri nurodoma Komisijos darbuotojų pareigybių aprašymuose.

V SKYRIUS
INFORMACIJOS SAUGUMO VALDYMO PLANAVIMAS

17. ISVS taikymo sritis ir ribos nustatomos, atsižvelgiant į Komisijos veiklos sritis, informacijos svarbą ir naudojamų technologijų pobūdį.

18. Komisijos informacijos saugumo rizikos ir galimybės informacijos saugumo srityje valdomos šiais veiksmais:

18.1. apibrėžiant rizikos vertinimo būdus;

18.2. identifikuojant rizikas;

18.3. analizuojant ir įvertinant rizikas;

18.4. nustatant ir įvertinant rizikos pašalinimo galimybes;

18.5. parenkant rizikų valdymo tikslus ir rizikų valdymo priemonės;

18.6. vadovybei pritariant liekamajai rizikai.

19. Informacijos saugumo tikslai kiekvieniems metams nustatomi Komisijos vadovybės vertinamosios analizės metu, atsižvelgiant į informacijos saugumo valdymo prioritetines kryptis. Detalūs informacijos saugumo tikslų vertinimo rezultatai vertinami taip, kaip nustatyta informacijos apsaugos priemonių veiksmingumo matavimo procese, o rezultatai pateikiami informacijos apsaugos priemonių veiksmingumo matavimo žurnale.

VI SKYRIUS
INFORMACIJOS SAUGUMO VALDYMO SISTEMOS DOKUMENTAI

20. ISVS reglamentuoja šie dokumentai:

20.1. Informacijos saugumo valdymo sistemos politika (1 priedas);

20.2. Aprašas;

20.3. Komisijos veiklos gerinimo proceso aprašas, kuriame reglamentuotas vadovybės vertinamosios analizės procesas;

20.4. Komisijos informacijos saugumo ir kokybės vadybos sistemos audito proceso aprašas;

20.5. Informacijos saugumo incidentų valdymo tvarkos aprašas (2 priedas);

20.6. Rizikos vertinimo atlikimo Komisijoje taisyklės;

20.7. Komisijos informacijos saugumo valdymo sistemos taikomumo pareiškimas;

20.8. Informacijos žymėjimo ir priežiūros procedūra (3 priedas);

20.9. Informacijos saugumo išimčių valdymo procedūra (4 priedas);

20.10. Veiklos tęstinumo valdymo planas (5 priedas);

20.11. Informacijos apsaugos priemonių veiksmingumo matavimo procesas (6 priedas);

20.12. Komisijos informacijos apdorojimo priemonių naudojimo taisyklės;

21.Komisijos pirmininko ir Komisijos, kaip kolegialaus valdymo organo, patvirtinti teisės aktai ir įrašai valdomi, vadovaujantis Komisijos vidaus darbo tvarkos taisyklių, patvirtintų Komisijos pirmininko 2013 m. gruodžio 31 d. įsakymo Nr. O1-104 „Dėl vidaus darbo tvarkos taisyklių patvirtinimo“, nuostatomis.

22. Elektroniniai duomenų įrašai (įvairių registrų forma) saugomi Komisijos informacinėse sistemose.

VII SKYRIUS
INFORMACIJOS SAUGUMO TAIKYMAS

23. Nustatyti informacijos saugumo tikslai ir pasirinktos informacijos saugumo valdymo priemonės yra įgyvendinamos, vadovaujantis Komisijos veiklos gerinimo proceso aprašo nustatyta tvarka.

24. Vadovaujantis rizikos vertinimo atlikimo Komisijoje taisyklėmis, parengiamas rizikos valdymo priemonių planas, kuriame numatomos informacijos apsaugos priemonės, joms reikalingi ištekliai, atsakomybės bei rizikos valdymo prioritetai.

25. Rizikos valdymo priemonių planas įgyvendinamas, pasiekiant numatytus valdymo tikslus, įskaitant finansavimo būdus bei pareigų ir atsakomybės paskirstymą.

26. Įgyvendinamos procedūros ir kitos informacijos saugumo valdymo priemonės, galinčios aptikti saugumo įvykius ir užtikrinti saugumo incidentų išsprendimą.

VIII SKYRIUS
INFORMACIJOS SAUGUMO VALDYMO SISTEMOS STEBĖSENA IR MATAVIMAS

27. Periodiškai turi būti atliekamos ISVS veiksmingumo peržiūros (įskaitant ISVS politikos ir tikslų atitikimo bei saugumo valdymo priemonių peržiūrą), atsižvelgiant į informacijos saugumo auditų rezultatus, įvykusius incidentus, veiksmingumo matavimo rezultatus bei visų suinteresuotųjų šalių pasiūlymus ir pastabas. ISVS veiksmingumas vertinamas, vadovaujantis Informacijos apsaugos priemonių veiksmingumo matavimo procesu.

28. Siekiant įsitikinti, kad saugumo reikalavimai įgyvendinami, turi būti matuojamas valdymo priemonių veiksmingumas.

29. Periodiškai turi būti atliekamas informacijos saugumo rizikos vertinimas, liekamosios rizikos ir numatytų priimtinos rizikos lygių analizė, atsižvelgiant į pokyčius Komisijoje.

IX SKYRIUS
INFORMACIJOS SAUGUMO VALDYMO SISTEMOS VIDAUS AUDITAS

30. Komisijos Vidaus audito skyrius atlieka ISVS vidaus auditą, kurio paskirtis – sistemingas ir nepriklausomas vertinimas, skirtas įvertinti, ar įdiegta ISVS atitinka Komisijos nustatytų procedūrų ir Komisijos pirmininko patvirtintų teisės aktų reikalavimus.

31. ISVS auditas atliekamas Vidaus audito skyriaus vidaus audito metodikoje nustatyta tvarka.

X SKYRIUS
KOMISIJOS VADOVYBĖS VERTINAMOJI INFORMACIJOS SAUGUMO VALDYMO SISTEMOS ANALIZĖ

32. Vadovybės vertinamoji ISVS analizė atliekama Komisijos veiklos gerinimo proceso aprašo nustatyta tvarka.

XI SKYRIUS
KOMISIJOS INFORMACIJOS SAUGUMO VALDYMO SISTEMOS TOBULINIMAS

33. Komisija nuolatos tobulina ISVS rezultatyvumą, įgyvendindama ISVS politiką ir tikslus, atlikdama ISVS vidaus auditus, nustatydama neatitiktis, vykdydama ISVS korekcinius veiksmus ir atlikdama vadovybės vertinamąja ISVS analizę.

34. Planuodama ISVS korekcinius veiksmus, Komisija vadovaujasi savo ir kitų organizacijų patirtimi.

35. ISVS neatitiktys ir korekciniai veiksmai valdomi, Komisijos veiklos gerinimo proceso apraše nustatyta tvarka.

XII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

36. Informacijos saugos įgaliotinis privalo ne rečiau kaip kartą per metus peržiūrėti Aprašą, jo priedus ir kitus susijusius dokumentus bei, iškilus poreikiui, inicijuoti reikiamus pakeitimus.

37. Komisijos darbuotojai, pažeidę šio Aprašą, jo priedų ar kitų Komisijos informacijos saugumą reglamentuojančių nuostatų reikalavimus, traukiami tarnybinėn ar drausminėn atsakomybėn.

38. Su šiuo Aprašu ir jo priedais yra supažindinami visi Komisijos darbuotojai.

_____

Valstybinės kainų ir energetikos kontrolės
komisijos Informacijos saugumo valdymo
sistemos aprašo
1 priedas

INFORMACIJOS SAUGUMO VALDYMO POLITIKA

1. Informacijos saugumo politika (toliau – Politika) – tai dokumentas, reglamentuojantis pagrindines informacijos saugumo nuostatas.

2. Informacija – tai Valstybinės kainų ir energetikos kontrolės komisijos (toliau – Komisija) veiklai strategiškai svarbus turtas, todėl informacijos praradimas, neteisėtas pakeitimas ar kiti neteisėti informacijos tvarkymo veiksmai gali sutrikdyti Komisijos veiklą. Atsižvelgiant į tai, ši Politika nustato pagrindines gaires, kuriomis, siekiant apsaugoti Komisijos informaciją, privalo vadovautis visi Komisijos pareigūnai, valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis (toliau – Darbuotojai), Tiekėjai ir kitos suinteresuotos šalys.

3. Informacijos saugumas apima tris pagrindinius aspektus:

- informacijos konfidencialumą – informacijos apsaugą nuo nesankcionuoto atskleidimo;
- informacijos vientisumą – informacijos apsaugą nuo nesankcionuoto ar atsitiktinio pakeitimo;
- informacijos pasiekiamumą – užtikrinimą, kad informacija prieinama tada, kai ji yra reikalinga.

4. Informacijos saugumo valdymo prioritetinės kryptys:

- užtikrinti tinkamą ir efektyvų informacijos saugumo valdymą ir išvengti veiklos sutrikdymo dėl informacijos konfidencialumo, vientisumo bei pasiekiamumo pažeidimų;
- užtikrinti atitiktį išoriniams reikalavimams;
- užtikrinti efektyvų rizikos valdymą ir tinkamų rizikos valdymo priemonių naudojimą, siekiant suvaldyti riziką iki priimtino lygio.

5. Pamatuojami informacijos saugumo tikslai kiekvieniems metams nustatomi Komisijos vadovybės vertinamosios analizės metu, atsižvelgiant į informacijos saugumo valdymo prioritetines kryptis.

6. Reikalavimai informacijos saugumui nustatomi:

- vadovaujantis suinteresuotų šalių keliamais reikalavimais bei lūkesčiais, išreikštais informacijos saugą reglamentuojančiuose teisės aktuose, duomenų teikimo ar kitokio pobūdžio sutartyse, išoriniais ir vidiniais informacijos keitimosi būdais (raštais, elektroniniais laiškais ir pan.);
- vadovaujantis Komisijos veiklos tikslais ir veiklos reikalavimais;
- vertinant informacijos saugumo riziką.

7. Komisijoje informacijos saugumo reikalavimų įgyvendinimas užtikrinamas ir valdomas nuosekliai planuojant, įgyvendinant, vertinant ir tobulinant informacijos saugumo valdymo sistemą (toliau – ISVS), vadovaujantis tarptautinio standarto ISO/IEC 27001 reikalavimais.

8. Komisijos vadovybė įsipareigoja:

- nustatyti informacijos saugumo valdymo tikslus;
- laikytis visų informacijos saugumo įsipareigojimų, reglamentuotų Europos Sąjungos ir Lietuvos Respublikos teisės aktuose bei sutartyse;
- užtikrinti efektyvų ISVS aprūpinimą reikiamais ištekliais;
- sudaryti sąlygas Komisijos pareigūnams, valstybės tarnautojams ir darbuotojams tobulinti žinias informacijos saugumo srityje.

9. Komisija nuolat gerina ISVS rezultatyvumą, įgyvendinama ISVS politiką ir tikslus, atlikdama ISVS vidaus auditus, nustatydama neatitiktis, vykdydama ISVS korekcinius veiksmus ir atlikdama vadovybės vertinamąją analizę.

10. ISVS taikoma:

- visuose Komisijos veiklos procesuose;

- visai Komisijoje naudojamai informacijai (nepriklausomai nuo jos formato ir saugojimo būdo);
- visiems Komisijos pareigūnams, valstybės tarnautojams ir darbuotojams;
- išorinių paslaugų Tiekėjams.

11. Politika platinama ISVS suinteresuotoms šalims joms prieinama ir suprantama forma.

12. Komisijos pareigūnai, valstybės tarnautojai ir darbuotojai yra susipažinę su Komisijos informacijos saugumo valdymo politika ir yra įsipareigoję jos laikytis.

13. Politika peržiūrima periodiškai, bet ne rečiau kaip kartą per metus.

_____

Valstybinės kainų ir energetikos kontrolės
komisijos Informacijos saugumo valdymo
sistemos aprašo
2 priedas

INFORMACIJOS SAUGUMO INCIDENTŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės kainų ir energetikos kontrolės komisijos (toliau – Komisija) informacijos saugumo incidentų valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja informacijos saugumo incidentų valdymo tvarką Komisijoje, siekiant užtikrinti Komisijos disponuojamos informacijos saugumą.

2. Komisijos informacijos saugumo incidentų valdymo tvarkos aprašas yra privalomas visiems Komisijos valstybės tarnautojams, pareigūnams ir darbuotojams, dirbantiems pagal darbo sutartis (toliau – darbuotojai).

3. Tiekėjams ir susijusioms šalims taikomas šio Aprašo 3 skyrius (Pranešimų teikimo apie informacijos saugumo įvykius tvarka), šio skyriaus nuostatai privalo būti pateikiami Tiekėjams ir susijusioms šalims kaip priedas prie sutarties.

4. Šiame Apraše vartojamos sąvokos:

ACER – Energetikos reguliavimo institucijų bendradarbiavimo agentūra.

Informacijos saugumas – apima informacijos konfidencialumo, vientisumo ir pasiekiamumo išsaugojimą.

Informacijos saugos įgaliotinis – Komisijos pirmininko įsakymu paskirtas Komisijos darbuotojas, atsakingas už informacijos saugumo valdymo Komisijoje įgyvendinimą ir palaikymą.

Informacijos saugumo įvykis – nustatytas sistemos, tarnybos ar tinklo įvykis, rodantis galimą informacijos saugumo politikos spragą ar informacijos saugumo priemonių triktį arba anksčiau nenumatytos situacijos, kuri gali būti susijusi su informacijos saugumu, atsiradimą.

Informacijos saugumo incidentas – vienas ar daugiau nepageidaujamų ir netikėtų informacijos saugumo įvykių, turinčių didelę tikimybę pakenkti Komisijos veiklai ir keliančių grėsmę informacijos saugumui.

IS – Informacinė sistema.

ISVS – Informacijos saugumo valdymo sistema.

Naudotojas – Komisijos darbuotojas, Tiekėjas, laikinai dirbantis konsultantas ar kitas Komisijoje dirbantis asmuo, įskaitant darbuotojus, dirbančius trečiosioms šalims, teisėtai tvarkančius Komisijos informaciją, kuriems suteikta priėjimo prie Komisijos informacijos ir/ar informacinių sistemų teisė naudotis IS ištekliais numatytoms funkcijoms atlikti.

Vadovybės vertinamoji ISVS analizė – tai vadovybės atliekamas visapusiškas veiklos nagrinėjimas, nustatantis ISVS efektyvumą, atitiktį reikalavimams bei numatantis galimus ISVS tobulinimo veiksmus.

II SKYRIUS
FUNKCIJOS IR ATSAKOMYBĖS

5. Už informacijos saugumo įvykių/informacijos saugumo incidentų valdymą Komisijoje atsakingi šie darbuotojai:

5.1. Informacijos saugos įgaliotinis:

5.1.1. įvertina užregistruotus informacijos saugumo įvykius;

5.1.2. tiria informacijos saugumo incidentus;

5.1.3. perduoda informacijos saugumo incidentus atsakingiems darbuotojams, pagal kompetenciją nagrinėti;

5.1.4. analizuoja informacijos saugumo incidentų tyrimo metu nustatytą ir/ar iš atsakingų darbuotojų gautą informaciją;

5.1.5. teikia Vadovybės vertinamosios analizės posėdžio metu ataskaitas Komisijos vadovybei;

5.1.6. teikia rekomendacijas ir metodinę pagalbą informacijos saugumo gerinimui Komisijoje;

5.1.7. užtikrina, kad informacijos saugumo incidentų valdymo tvarka būtų gerai žinoma visiems Komisijos darbuotojams;

6. Informacijos saugos įgaliotinio laikino nebuvimo darbe metu jį pavaduoja kitas Komisijos pirmininko įsakymu paskirtas darbuotojas.

7. Naudotojai yra atsakingi už jiems nustatytos pareigos – pranešti apie bet kokį informacijos saugumo įvykį – tikslų vykdymą. Teisinė atsakomybė kiekvienam Komisijos darbuotojui, Tiekėjui ir trečiosios šalies atstovui taikoma individualiai – laikantis bendrų teisinės atsakomybės skyrimo principų: priklausomai nuo vykdomų funkcijų, atliekamo darbo ar teikiamų paslaugų svarbos, padarytos žalos dydžio bei masto.

8. Naudotojai privalo teikti informacijos saugos įgaliotiniui visą su informacijos saugumo įvykiais ir incidentais susijusią informaciją kaip galima greičiau nuo jų atsiradimo momento.

III SKYRIUS
PRANEŠIMŲ TEIKIMO APIE INFORMACIJOS SAUGUMO ĮVYKIUS TVARKA

9. Naudotojai, pastebėję informacijos saugumo įvykius ar informacijos saugumo silpnąsias vietas, privalo nedelsiant pranešti apie tai elektroniniu paštu informacijos saugos įgaliotiniui Saugos.igaliotinis@regula.lt bei apie jį informuoti ir savo tiesioginį vadovą. Įvykiai apie kuriuos reikia pranešti gali būti tokie, kaip:

9.1. informacijos saugumo politikos ar reikalavimų pažeidimai;

9.2. techninės ir (ar) programinės įrangos sutrikimai ir (ar) netikėti apkrovos pasikeitimai dėl neaiškių priežasčių;

9.3. fizinės saugos priemonių pažeidimai;

9.4. vagystės;

9.5. pastebėti įtartini lankytojų veiksmai;

9.6. asmens duomenų saugumo pažeidimai;

9.7. kitų asmenų pranešimai apie galimą grėsmę ir informacijos saugumo pažeidimus, įskaitant ir anoniminius pranešimus;

9.8. kiti įvykiai, galintys turėti įtakos informacijos saugumui.

10. Pranešimus apie pastebėtus informacijos saugumo įvykius galima pateikti ir:

10.1. telefonu;

10.2. tiesiogiai atvykus į informacijos saugos įgaliotinio darbo vietą;

10.3. pranešimai gali būti pateikiami ir anonimiškai.

IV SKYRIUS
INFORMACIJOS SAUGUMO ĮVYKIŲ IR INCIDENTŲ REGISTRAVIMAS

11. Informacijos saugos įgaliotinis, gavęs pranešimą arba pats pastebėjęs informacijos saugumo pažeidimą, užregistruoja jį informacijos saugumo įvykių ir incidentų registre, kuriame turi būti nurodyta data ir laikas, įvykio aprašymas, sprendimas ar įvykis priskiriamas informacijos saugumo incidentui, kategorija ir numatomas incidento išsprendimo laikas, tipas, atsakingas už incidento sprendimą asmuo, žalos aprašymas, įvykio priežastis, incidento sprendimo aprašymas, informacija apie įrodymus (jei reikia), incidento išsprendimo data.

12. Informacijos saugos įgaliotinis nusprendžia, ar užregistruotas informacijos saugumo įvykis priskiriamas informacijos saugumo incidentui.

13. Informacijos saugos įgaliotinis taip pat registruoja informacijos saugumo incidentus, kai informacijos apsaugos priemonių veiksmingumo matavimo rezultatai nustatyti kaip pavojingi (žr. Informacijos apsaugos priemonių veiksmingumo matavimo procesas).

14. Informacijos saugumo įvykiai turi būti stebimi, o informacijos saugumo incidentai – tiriami.

V SKYRIUS
INFORMACIJOS SAUGUMO INCIDENTŲ TYRIMO TVARKA

15. Gavęs pranešimą apie naują užregistruotą informacijos saugumo įvykį, Informacijos saugos įgaliotinis atlieka pirminį informacijos saugumo įvykio įvertinimą. Pirminio įvertinimo metu nustatoma, ar informacijos saugumo įvykis yra informacijos saugumo incidentas ir gali kelti grėsmę informacijos saugumui:

15.1. jei informacijos saugumo įvykis negali kelti grėsmės informacijos saugumui, jis uždaromas, fiksuojant, kad buvo gautas pranešimas apie informacijos saugumo įvykį, bet tolimesnis informacijos saugumo įvykio tyrimas neatliekamas. Apie saugumo incidentą pranešęs Naudotojas informuojamas apie saugumo įvykio uždarymą su komentaru;

15.2. jei informacijos saugumo įvykis gali kelti grėsmę informacijos saugumui, atliekamas antrinis įvertinimas.

16. Antrinio įvertinimo metu:

16.1. informacijos saugos įgaliotinis nustato informacijos saugumo incidento tipą. Galimi keturi informacijos saugumo incidentų tipai:

16.1.1. Elektroninės informacijos saugumo incidentas – tai įvykis, veiksmas ar neveikimas, kuris sukelia ar gali sukelti neteisėtą prisijungimą ar sudaryti sąlygas neteisėtai prisijungti prie IS ar elektroninių ryšių tinklo, sutrikdyti ar pakeisti (įskaitant valdymo perėmimą) IS ar elektroninių ryšių tinklo veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninius duomenis, panaikinti ar apriboti galimybę naudotis elektroniniais duomenimis, gali sudaryti sąlygas pasisavinti, paskelbti, platinti ar kitaip panaudoti neviešus elektroninius duomenis tokios teisės neturintiems asmenims;

16.1.2. Neelektroninės informacijos saugumo incidentas – tai įvykis, veiksmas ar neveikimas, susijęs su kitų formų informacija (spausdintiniai, rašytiniai dokumentai ir jų kopijos ir t. t.). Taip pat tai įvykiai, susiję su fizine apsauga, kai galėjo kilti Komisijoje disponuojamos informacijos ar jos dalies praradimo bei sugadinimo rizika;

16.1.3. Kibernetinis incidentas – įvykis ar veikla, kuri sukelia ar gali sukelti neteisėtą prisijungimą ar sudaryti sąlygas neteisėtai prisijungti prie IS, sutrikdyti ar pakeisti IS veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją ar elektroninius duomenis panaikinti ar apriboti galimybę naudotis elektronine informacija ar elektroniniais duomenimis, taip pat sudaryti sąlygas pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją ar elektroninius duomenis tokios teisės neturintiems asmenims.

16.1.4. Informacijos saugumo incidentas, susijęs su asmens duomenų saugumo pažeidimu.

16.2. Informacijos saugos įgaliotinis saugumo incidentą pagal kompetenciją sprendžia pats arba, atsižvelgdamas į informacijos saugumo incidento tipą, pasitelkia reikiamus specialistus iš kitų Komisijos struktūrinių padalinių arba išorės ekspertus, atlikti tolimesnį informacijos saugumo incidentų tyrimą.

17. Atliekant tolesnį informacijos saugumo incidento tyrimą:

17.1. informacijos saugumo incidentui priskiriama pavojingumo kategorija, pagal žemiau pateiktus kriterijus:

17.1.1. I kategorijos – kai informacijos saugumo incidentas sukelia neigiamas pasekmes visai Komisijai, kai dėl tokio informacijos saugumo incidento gali sutrikti visų IS veikla;

17.1.2. II kategorijos – kai saugumo incidentas kenkia vienai ar kelioms Komisijos funkcijoms, daro įtaką daugiau nei vienam Komisijos struktūriniam padaliniui, yra susijęs su Komisijos valstybinėmis IS, arba su informacijos mainais su ACER;

17.1.3. III kategorijos – kai informacijos saugumo incidentas iš esmės nedaro įtakos Komisijos veiklai arba su ja susijęs neženkliai, daro įtaką ne daugiau nei vienam Komisijos struktūriniam padaliniui;

17.2. Informacijos saugos įgaliotinis, atsižvelgdamas į informacijos saugumo incidento kategoriją:

17.2.1. nusprendžia, kokia seka ir apimtimi vykdyti reagavimo į incidentą veiklas:

17.2.1.1. neatidėliotinus veiksmus;

17.2.1.2. faktinių aplinkybių (įrodymų) nustatymą;

17.2.1.3. komunikaciją;

17.2.2. užtikrina vykdomų operacijų atkūrimą ir išlaikymą:

17.2.2.1. reikiamu lygiu;

17.2.2.2. per atitinkamą laiko tarpą;

17.2.2.3. laikantis taikomų procedūrų, leidžiančių per reikiamą laiką atkurti ir atstatyti veiklos operacijas bei informacijos parengtumą;

17.2.2.4. nustatytu priimtinu informacijos ir paslaugų praradimo lygiu.

17.2.3. taiko atitinkamas priemones, apimančias:

17.2.3.1. incidento priežasties nustatymą ir analizę;

17.2.3.2. incidentų suvaldymą;

17.2.3.3. pataisos veiksmų planavimą ir įgyvendinimą, siekiant išvengti informacijos saugumo incidento pasikartojimo;

17.2.3.4. ryšio palaikymą su asmenimis, kurių darbas susijęs su informacijos saugumo incidentų sukeltų nesklandumų panaikinimu;

17.2.4. sprendžia, ar informacijos saugumo incidentas yra valdomas:

17.2.4.1. jei nustatoma, kad informacijos saugumo incidento negalima suvaldyti per laikotarpį nuo vienos dienos iki savaitės ir/arba informacijos saugumo incidentas turi/gali turėti dideles neigiamas pasekmes Komisijai, šaukiama Veiklos tęstinumo valdymo grupė ir priimamas sprendimas dėl nenumatytos situacijos skelbimo.

18. Jei nenumatytos situacijos nusprendžiama neskelbti, Veiklos tęstinumo valdymo grupė numato priemones informacijos saugumo incidentui valdyti;

19. Nusprendus skelbti nenumatytą situaciją, ji valdoma pagal Komisijos Bendrąjį veiklos tęstinumo planą, patvirtintą Komisijos pirmininko įsakymu.

20. Atlikus informacijos saugumo incidento tyrimą, jį koordinavęs darbuotojas privalo vidiniame Komisijos tinklapyje, tam skirtoje skiltyje, paviešinti komentarą apie informacijos saugumo incidento priežastis, priemones/veiksmus, kurių buvo imtasi, siekiant užkirsti kelią informacijos saugumo incidentui pasikartoti ateityje. Informacijos saugumo incidentų sprendėjų komentarai saugomi Komisijos tinklapyje, tam skirtoje skiltyje ir elektroniniu paštu siunčiami susipažinti registravusiam Naudotojui.

21. Informacijos saugos įgaliotinis periodiškai, kartą per mėnesį peržiūri užregistruotus informacijos saugumo incidentus.

22. Informacijos saugumo incidentų analizės pagrindu Informacijos saugos įgaliotinis gali inicijuoti neeilinį informacijos saugumo rizikos vertinimą.

23. Incidentų analizės duomenys analizuojami ir iš jų mokomasi, siekiant sumažinti ateityje įvyksiančių informacijos saugumo incidentų įtaką ir (ar) tikimybę.

VI SKYRIUS
INFORMACIJOS APIE INFORMACIJOS SAUGUMO INCIDENTUS SAUGOJIMAS IR ATASKAITŲ TEIKIMAS

24. Visi pranešimai apie informacijos saugumo įvykius ir informacijos saugumo incidentus, bei informacijos saugumo incidentų tyrimo metu surinkta medžiaga saugoma Komisijos serveryje, o informacija pateikiama tinklapyje, tam skirtoje skiltyje.

25. Du kartus per metus, iki einamųjų metų vasario 15 d. ir iki einamųjų metų rugpjūčio 15 d., Informacijos saugos įgaliotinis teikia Vadovybės vertinamosios analizės posėdžiui per praėjusį pusmetį nustatytų informacijos saugumo incidentų apibendrintas ataskaitas su komentarais apie tai ar kartojasi informacijos saugumo incidentai, ar kartojasi jų atsiradimo priežastys bei siūlymais, kaip

mažinti galimų informacijos saugumo incidentų atsiradimo riziką, apsvarstant galimybę tam skirti papildomus išteklius.

VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

26. Šis Aprašas tikrinamas ir peržiūrimas pagal poreikį (po rizikos analizės ar informacinių technologijų saugumo atitikties vertinimo atlikimo arba įvykus esminiams organizaciniams, sisteminiams ar kitiems informacinės sistemos pokyčiams), bet ne rečiau kaip vieną kartą per kalendorinius metus.

_____

Valstybinės kainų ir energetikos kontrolės komisijos Informacijos saugumo valdymo sistemos aprašo
3 priedas

INFORMACIJOS ŽYMĖJIMO IR PRIEŽIŪROS PROCEDŪRA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Procedūra nustato Valstybinėje kainų ir energetikos kontrolės komisijoje (toliau – Komisija) tvarkomos informacijos klasifikavimo ir žymėjimo tvarką, siekiant užtikrinti, kad informacija bus tinkamai identifikuota ir apsaugota pagal klasifikaciją, atitinkančią Komisijos poreikius.

2. Procedūra taikoma visuose Komisijos skyriuose, visose veiklos srityse, bet kokios formos (elektroninė ar popierinė) Komisijoje tvarkomai informacijai, išskyrus įslaptintai informacijai, jos laikytis privalo visi Komisijos valstybės tarnautojai, pareigūnai ir darbuotojai, dirbantys pagal darbo sutartis (toliau – Darbuotojai).

3. Šioje procedūroje vartojamos sąvokos:

ACER – Energetikos reguliavimo institucijų bendradarbiavimo agentūra.

Informacijos saugumas – apima informacijos konfidencialumo, vientisumo ir pasiekiamumo išsaugojimą.

ISVS – Informacijos saugumo valdymo sistema.

Konfidencialumas – savybė, nusakanti tai, kad informacija nebus prieinama ar pateikiama neįgaliotiems fiziniams ar juridiniams asmenims arba procesams.

Konfidenciali informacija – tai duomenys (informacija), kurie turi vertę dėl to, kad jos nežino tretieji asmenys ir ji negali būti laisvai prieinama. Konfidenciali informacija gali būti išsaugota dokumentuose, kompiuterio diskuose, diskeliuose, kitose informacijos laikmenose, brėžiniuose, schemose ir bet kokiose kitose informacijos (duomenų) tvarkymo (saugojimo) priemonėse. Konfidenciali informacija taip pat gali būti ir žodinė, t. y. egzistuojanti žmogaus atmintyje ir neišreikšta jokia materialia forma.

Konfidencialios informacijos atskleidimas – darbuotojo, kuriam konfidenciali informacija buvo patikėta arba tapo žinoma dėl jo tarnybos ar darbo funkcijų, veikimas ar neveikimas, dėl kurio konfidenciali informacija tapo žinoma (arba sudaromos sąlygos ją sužinoti) bent vienam asmeniui, kuris neturi teisės susipažinti su šia informacija. Asmenimis, kurie neturi teisės susipažinti su konfidencialia informacija nėra laikomos Lietuvos Respublikos ar kitų valstybių institucijos, įstaigos, organizacijos, kurioms Komisija teisės aktų ar tarpusavio susitarimų pagrindu teikia su savo veikla susijusią informaciją.

Pasiekiamumas – informacijos savybė, reiškianti, kad informacija gali būti tvarkoma reikiamu metu.

Vientisumas – informacijos savybė, reiškianti, kad informacija nebuvo atsitiktiniu ar neteisėtu būdu pakeista ar sunaikinta.

II SKYRIUS
FUNKCIJOS IR ATSAKOMYBĖS

4. Informacijos saugos įgaliotinis:

4.1. kontroliuoja, kad informacija būtų žymima pagal nustatytus reikalavimus;

4.2. supažindina darbuotojus su informacijos klasifikavimo ir žymėjimo reikalavimais.

5. Informacinių išteklių valdytojai:

5.1. pateikia informacijos saugumo įgaliotiniui informaciją apie jų valdomos informacijos kategoriją;

5.2. atsako už jų valdomos informacijos kategorijos nustatymą;

5.3. nustato jų valdomos informacijos tinkamo žymėjimo ir priežiūros reikalavimus.

6. Skyrių vedėjai:

6.1. organizuoja prieigos suteikimą skyrių darbuotojams prie reikalingos informacijos;

6.2. pateikia atsakingiems darbuotojams viešo naudojimo informaciją skelbimui internetiniame Komisijos puslapyje, pranešimuose spaudai ir pan.

7. Komisijos pirmininkas:

7.1. tvirtina konfidencialios informacijos sąrašą;

7.2. sprendžia dėl prieigos suteikimo darbuotojams prie reikalingos informacijos.

III SKYRIUS
INFORMACIJOS KLASIFIKAVIMAS

8. Komisijoje naudojama informacija klasifikuojama į šias kategorijas: vieša, vidinio naudojimo, asmens duomenys, konfidenciali ir padidinto konfidencialumo.

9. Vieša informacija – informacija, kurią Komisija skelbia viešai savo internetiniame puslapyje, pranešimuose spaudai ir pan.

10. Vidinio naudojimo informacija – visa Komisijoje tvarkoma informacija, kuri nepriskirta konfidencialiai, padidinto konfidencialumo, asmens duomenims ar viešai informacijai.

11. Asmens duomenys – bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta.

12. Konfidenciali informacija:

12.1. tarnybos ar darbo metu sužinotos fizinių ir juridinių asmenų komercinės, gamybinės ir technologinės paslaptys, kaip jos apibrėžiamos pagal Lietuvos Respublikos civilinį kodeksą;

12.2. informacija, kuriai pagal vidinę juridinių asmenų tvarką ar sudarytus sandorius nustatytas konfidencialios informacijos statusas;

12.3. žinios apie Komisijoje esančius kompiuterius, kompiuterinės įrangos sistemas, kompiuteriuose sukaupta informacija, informacija apie Komisijoje veikiančias informacines sistemas (Dokumentų valdymo sistema („@vilys"), duomenų surinkimo ir analizės informacinė sistema (DSAIS), intranetas bei kitos teisėtai veikiančios sistemos ir jose esanti informacija, bendrojo informacijos telefono, apsaugos ir signalizacijos informacija.

13. Padidinto konfidencialumo informacija – iš Energetikos reguliavimo institucijų bendradarbiavimo Agentūros (ACER) gaunama ir/ar jai teikiama informacija, įgyvendinant Europos Parlamento ir Tarybos 2011 m. spalio 25 d. reglamento (ES) Nr. 1227/2011 dėl didmeninės energijos rinkos vientisumo ir skaidrumo 7 str. 2 d. ir 16 str. nuostatas.

IV SKYRIUS
INFORMACIJOS ŽYMĖJIMAS IR TVARKYMAS

14. Komisijoje žymima tik konfidenciali ir padidinto konfidencialumo informacija.

15. Konfidenciali informacija žymima ir tvarkoma, laikantis Komisijos vidaus darbo tvarkos taisyklių XVI skyriuje nurodytų nuostatų.

16. Asmens duomenys tvarkomi pagal Komisijos vidaus darbo tvarkos taisyklių XVII skyriuje nurodytas nuostatas.

17. Padidinto konfidencialumo popierinė informacija žymima uždedant žymą „Padidinto Konfidencialumo" viršutiniame kairiame lapo kampe. Elektroninė informacija turi būti žymima šiais būdais:

17.1. tekstinio redagavimo programomis (word formatu ir pan.) rengiami dokumentai, uždedant žymą viduje taip pat, kaip popierinę informaciją;

17.2. elektroninės rinkmenos pavadinimo gale arba pradžioje įrašant „Padidinto konfidencialumo".

18. Nesant techninių galimybių, kitais atvejais elektroninė padidinto konfidencialumo informacija gali būti nežymima, tačiau turi būti aiškiai nurodyta informacijos tvarkymo vieta, pavyzdžiui, informacinė sistema.

19. Visais atvejais, tai, kad informacija nepažymėta kaip konfidenciali ar padidinto konfidencialumo, nereiškia, kad ji yra vidinio naudojimo ar vieša informacija ir jai netaikomi nustatyti tvarkymo reikalavimai, išskyrus informaciją, kuri apibrėžta Lietuvos Respublikos energetikos įstatymo 25 straipsnio 5 dalyje, kuri numato, kad energetikos įmonių informacija apie sąnaudas, susijusias su teisės aktų nustatyta tvarka licencijuojama veikla arba su veikla, kuriai taikomos valstybės reguliuojamos kainos, yra vieša.

20. Esant neaiškumui, dokumentų rengėjas ar gavėjas konsultuojasi su informacinio ištekliaus valdytoju, kuris yra atsakingas už atitinkamos informacijos kategorijos nustatymą.

21. Asmens duomenys, vidinio naudojimo ir vieša informacija nėra žymima.

22. Padidinto konfidencialumo informacija yra saugoma ir be rašytinio Komisijos pirmininko sutikimo draudžiama atskleisti ar pranešti ją tretiesiems asmenims, išskyrus teisės aktuose nustatytais atvejais. Darbuotojams prieiga prie šios informacijos suteikiama tik tokios apimties, kurios reikia darbui atlikti.

23. Prieigą prie asmens duomenų, konfidencialios, padidinto konfidencialumo ir vidinio naudojimo informacijos inicijuoja skyrių vedėjai.

24. Jeigu su dokumentu, kuriame tam tikros jo dalys ar priedai yra padidinto konfidencialumo, turi susipažinti asmuo, kuris neturi teisės matyti šią informaciją, jam pateikiama dokumento kopija be padidinto konfidencialumo informacijos (pvz., nepridedant priedų, puslapių, kuriuose yra padidinto konfidencialumo informacija arba, darant kopiją, uždengiant padidinto konfidencialumo informaciją, arba ištrinant informaciją, jei tai elektroninė rinkmena).

25. Padidinto konfidencialumo informaciją draudžiama siųsti elektroniniu paštu ar kitomis elektroninėmis priemonėmis (pvz. e-pristatymas), išskyrus tuos atvejus, kai tai yra būtina ir nėra kitų galimybių. Jei būtina siųsti padidinto konfidencialumo informaciją, ji turi būti šifruojama.

26. Keičiamose laikmenose perduodant padidinto konfidencialumo informaciją, ji turi būti šifruojama.

27. Jei padidinto konfidencialumo informacijos iššifravimui informacijos gavėjui bus reikalingas slaptažodis ar raktas, jis turi būti perduodamas atskirai nuo padidinto konfidencialumo informacijos ir kitu būdu nei buvo perduota padidinto konfidencialumo informacija.

28. Padidinto konfidencialumo informacija negali būti laikoma tretiesiems asmenims lengvai prieinamoje vietoje, pavyzdžiui, ant stalo (išskyrus atvejus, kai su ja tuo metu dirbama). Padidinto konfidencialumo informacija turi būti laikoma, esant galimybei, rakinamuose stalčiuose ar spintose, seifuose. Jei į kabinetą užeina asmuo, kuris neturi teisės susipažinti su padidinto konfidencialumo ar konfidencialia informacija, dokumentai, kuriuose yra konfidencialios informacijos ir su kuriais tuo metu buvo dirbama, užverčiami.

29. Prieš įrangai patenkant į patalpas, kuriose saugoma padidinto konfidencialumo informacija, ji turi būti patikrinta atsakingo darbuotojo. Turi būti tikrinama, ar įranga atitinka reikiamą konfigūraciją ir komplektaciją.

30. Jei įranga, kurioje yra padidinto konfidencialumo informacijos, turi būti perkeliama į kitas patalpas, kuriose yra mažesnis apsaugos lygis, iš įrangos turi būti pašalinta padidinto konfidencialumo informacija.

31. Į patalpas, kuriose saugoma padidinto konfidencialumo informacija galima patekti tik asmenims, dirbantiems su padidinto konfidencialumo informacija, turi būti kontroliuojama prieiga, naudojamos vaizdo stebėjimo priemonės, įrengta atskira signalizacijos zona.

32. Patalpose, kuriose saugoma padidinto konfidencialumo informacija turi būti dirbama taip, kad ekranas būtų pastatytas kuo toliau nuo lango, kad nebūtų galimybės pašaliniams asmenims pamatyti laikomą informaciją.

33. Jeigu buvo padarytos padidinto konfidencialumo informacijos popierinės kopijos, pasibaigus darbui ar kai jos tampa nebereikalingos, jos turi būti sunaikinamos.

34. Jei padidinto konfidencialumo informacija siunčiama paštu, ji turi būti siunčiama registruotu paštu ar naudojantis kurjerių paslaugomis. Tiek padidinto konfidencialumo, tiek konfidenciali, tiek asmens duomenys, tiek vidinio naudojimo informacija siunčiant turi būti supakuota taip, kad siuntimo metu negalima būtų susipažinti su šia informacija.

35. Vieša informacija skelbiama Komisijos internetiniame puslapyje, pranešimuose spaudai ir pan. Už viešos informacijos pateikimą, jos teisingumą ir tinkamumą atsakingi skyrių vedėjai pagal skyrių funkcijas.

36. Vidinio naudojimo informaciją draudžiama atskleisti tretiesiems asmenims be Komisijos pirmininko sutikimo.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

37. Ši Procedūra tikrinama ir peržiūrima pagal poreikį, bet ne rečiau kaip vieną kartą per kalendorinius metus.

38. Informacijos saugos įgaliotinis gali inicijuoti Procedūros pakeitimus šiais atvejais:

38.1. gavus iš skyriaus vedėjų arba informacinių išteklių valdytojų informaciją apie konfidencialios ar padidinto konfidencialumo informacijos papildymo ar pakeitimo poreikį;

38.2. atsiradus poreikiui papildyti informacijos klasifikavimą papildomais požymiais;

38.3. pasikeitus teisės aktų, reglamentuojančių informacijos saugumą, reikalavimams ar sutartiniams informacijos saugumo įsipareigojimams.

_____

Valstybinės kainų ir energetikos kontrolės
komisijos Informacijos saugumo valdymo
sistemos aprašo
4 priedas

INFORMACIJOS SAUGUMO IŠIMČIŲ VALDYMO PROCEDŪRA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės kainų ir energetikos kontrolės komisijos (toliau – Komisija) informacijos saugumo išimčių valdymo procedūra (toliau – Procedūra) reglamentuoja išimčių iš nustatytų informacijos saugumo reikalavimų valdymo tvarką Komisijoje, siekiant užtikrinti Komisijos disponuojamos informacijos saugumą.

2. Ši procedūra taikoma visiems ISVS dokumentacijoje nustatytiems reikalavimams, visiems Komisijos valstybės tarnautojams, pareigūnams ir darbuotojams, dirbantiems pagal darbo sutartis (toliau – Darbuotojai).

3. Visi Komisijos darbuotojai privalo laikytis nustatytų informacijos saugumo reikalavimų, taisyklių, procedūrų ir elgtis su informaciniais ištekliais taip, kaip nustatyta, tačiau išskirtiniais atvejais, kai neįmanoma dėl įvairių priežasčių atitikti nustatytų reikalavimų, gali būti nustatytos išimtys. Tokiais atvejais išimtys turi būti dokumentuotos ir tvirtinamos, vadovaujantis šia Procedūra.

4. Išimtys nustatytiems informacijos saugumo reikalavimams gali būti suteikiamos, susidarius žemiau aprašytoms situacijoms:

4.1. laikinos išimtys, kai:

4.1.1. laikymasis nustatytų reikalavimų gali sutrukdyti pagrindinių veiklų vykdymą;

4.1.2. atitiktis neįmanoma dėl techninių trukdžių;

4.2. ilgalaikės išimtys, kai:

4.2.1. atitikimas trikdytų veiklos procesus;

4.2.2. kai atitiktis sukelia didesnius finansinius nuostolius nei galima rizika, dėl kurios nustatytas reikalavimas.

5. Išimtys gali būti susijusios su:

5.1. prieigos valdymu (paskyros, naudojamos paslaugų teikimui pradėti, paskyros programose, skirtos gauti prieigai prie paslaugų už programos ribų ir kt.);

5.2. slaptažodžių naudojimu;

5.3. programinės įrangos diegimais (išimtys turi būti patvirtintos sistemos savininko);

5.4. nepriimtina rizika (nepriimtinos rizikos atvejams, nepatenkantiems į informacijos saugumo taikymo sritį ir rizikos atvejais, kurių įgyvendinimo laikotarpis ilgesnis nei vieneri metai);

5.5. kitais informacijos saugumo reikalavimais.

6. Šioje Procedūroje vartojamos sąvokos:

Darbuotojai – Komisijos valstybės tarnautojai, pareigūnai ir darbuotojai, dirbantys pagal darbo sutartis.

Informacijos saugumas – apima informacijos konfidencialumo, vientisumo ir pasiekiamumo išsaugojimą.

Informacijos saugos įgaliotinis – Komisijos pirmininko įsakymu paskirtas Komisijos darbuotojas, atsakingas už informacijos saugumo valdymo Komisijoje įgyvendinimą ir palaikymą.

Informacijos saugumo įvykis – nustatytas sistemos, tarnybos ar tinklo įvykis, rodantis galimą informacijos saugumo politikos spragą ar informacijos saugumo priemonių triktį arba anksčiau nenumatytos situacijos, kuri gali būti susijusi su informacijos saugumu, atsiradimą.

Informacijos saugumo incidentas – vienas ar daugiau nepageidaujamų ir netikėtų informacijos saugumo įvykių, turinčių didelę tikimybę pakenkti veiklai ir keliančių grėsmę informacijos saugumui.

IS – Informacinė sistema.

ISVS – Informacijos saugumo valdymo sistema.

Naudotojas – Komisijos darbuotojas, tiekėjas, laikinai dirbantis konsultantas ar kitas Komisijoje dirbantis asmuo, įskaitant darbuotojus, dirbančius trečiosioms šalims, teisėtai tvarkančius Komisijos informaciją, kuriems suteikta priėjimo prie Komisijos informacijos ir/ar informacinių sistemų teisė naudotis informacinės sistemos ištekliais numatytoms funkcijoms atlikti.

II SKYRIUS
FUNKCIJOS IR ATSAKOMYBĖS

7. Už informacijos saugumo išimčių valdymą Komisijoje atsakingi šie darbuotojai:

7.1. informacijos saugos įgaliotinis:

7.1.1. peržiūri ir patvirtina (vizuoja teigiamai) arba atmeta (vizuoja neigiamai) išimčių prašymus;

7.1.2. jei reikia, paprašo papildomos informacijos dėl išimties;

7.1.3. jei reikia, tariasi dėl išimties suteikimo su Komisijos pirmininku;

7.1.4. nustato ar reikalingos papildomos išimties peržiūros;

7.1.5. dokumentuoja specialias sąlygas ar reikalavimus išimties suteikimui;

7.1.6. seka išimčių prašymus ir peržiūri juos bent kartą per metus;

7.1.7. nustato išimčių tinkamumą;

7.1.8. inicijuoja išimties atšaukimą, susidūrus su incidentu ar pažeidimo atveju;

7.1.9. yra atsakingas už išimčių valdymo procedūrą ir prireikus inicijuoja pakeitimus.

7.2. asmuo, pateikiantis prašymą suteikti išimtį:

7.2.1. teikia užpildytą išimties prašymo formą pagal Procedūros III skyriaus reikalavimus, patvirtinti (vizuoti) skyriaus vedėjui, informacijos saugos įgaliotiniui, Administracijos direktoriui ir Komisijos pirmininkui.

7.2.2. jei reikia, tariasi su informacijos saugos įgaliotiniu dėl prašymo pildymo;

7.2.3. užtikrina pateiktos informacijos tikslumą.

7.3. Skyriaus vedėjas peržiūri ir tvirtina (vizuoja teigiamai) arba atmeta (vizuoja neigiamai) prašymus dėl išimčių, susijusių su jo valdomais ištekliais;

7.4. Administracijos direktorius peržiūri ir tvirtina (vizuoja teigiamai) arba atmeta (vizuoja neigiamai) prašymus dėl išimčių, susijusių su jo valdomais ištekliais;

7.5. Komisijos pirmininkas:

7.5.1. peržiūri ir tvirtina (vizuoja) arba atmeta (vizuoja neigiamai) prašymus dėl išimčių, susijusių su jo valdomais ištekliais;

7.5.2. yra atsakingas už riziką, susijusią su išimties suteikimu.

III SKYRIUS
IŠIMČIŲ VALDYMO TVARKA

8. Prieš pateikiant prašymą išimčiai asmuo, pateikiantis prašymą išimčiai, turi įvertinti riziką, t. y. turi būti identifikuotos su išimtimi susijusios grėsmės ir pažeidžiamumai, grėsmių tikimybė ir galimas nuostolis, taip pat pasiūlytos priemonės rizikai valdyti.

9. Prašymai išimtims turi būti siunčiami patvirtinti (vizuoti) skyriaus vedėjui, informacijos saugos įgaliotiniui, Administracijos direktoriui ir Komisijos pirmininkui per Komisijos naudojamą dokumentų valdymo sistemą „Avilys“ (toliau – DVS) nuosekliai. Prašyme turi būti nurodyta žemiau išvardinta informacija (išimties prašymo forma pateikta Procedūros priede):

9.1. reikalavimas, kuriam prašoma išimties;

9.2. priežastis, dėl kurios prašoma išimties;

9.3. situacijos, kuri įvyks suteikus išimtį, aprašymas;

9.4. su reikalavimo nesilaikymu susijusios neatitikties rizikos įvertinimas;

9.5. pasiūlytas rizikos, susijusios su išimtimi, valdymo būdas;

9.6. papildoma informacija;

9.7. tikėtina išimties trukmė (ilgiausias periodas 1 metai);

9.8. papildoma informacija.

10. Informacijos saugos įgaliotinis, Administracijos direktorius ir Komisijos pirmininkas turi susipažinti su visais išimčių prašymais.

11. Informacijos saugos įgaliotinis gali nuspręsti netvirtinti (vizuoti neigiamai) pateikto išimties prašymo, jei mano, kad tokios išimties suteikimas gali pakenkti informacijos saugumui.

12. Išimčių, kurios kelia didelę riziką Komisijai ir joms nėra numatytų riziką mažinančių priemonių, prašymai negali būti patvirtinami (vizuojami teigiamai).

13. Išimčių pratęsimai negali būti automatiškai patvirtinami, turi būti pateiktas atskiras prašymas.

14. Kai tam tikros rūšies išimtis buvo suteikta, būsimos tos pačios rūšies užklausos gaus tą patį sprendimą, nebent atsižvelgiant į ypatingas aplinkybes, gali būti priimtas kitoks sprendimas.

15. Jei kartojasi prašymai patvirtinti tos pačios rūšies išimtis, tai gali reikšti, kad atitinkami standartai turi būti koreguojami taip, kad išimtis būtų norma. Informacijos saugos įgaliotinis tokiais atvejais gali inicijuoti reikalavimo, procedūros ar proceso keitimą.

16. Prašymai dėl išimties gali būti atšaukti saugumo incidento ar politikos pažeidimo atveju, vadovaujantis Informacijos saugumo incidentų valdymo tvarkos aprašu.

IV SKYRIUS
IŠIMČIŲ VALDYMO PROCESAS

17. Išimties prašantis Darbuotojas kreipiasi dėl išimties suteikimo, užpildydamas išimties prašymo formą ir pateikdamas ją III skyriuje nustatyta tvarka.

18. Informacijos saugos įgaliotinis surenka visą reikalingą informaciją ir nusprendžia, ar reikia konsultuotis su Komisijos pirmininku, ir pateikia rekomendaciją patvirtinti (vizuoti teigiamai) arba atmesti prašymą (vizuoti neigiamai).

19. Informacijos saugos įgaliotinis susisiekia su išimties prašančiu Darbuotoju, jei reikia papildomos informacijos.

20. Informacijos saugos įgaliotinis, Administracijos direktorius ir Komisijos pirmininkas patvirtina (vizuoja teigiamai) arba paneigia (vizuoja neigiamai) prašymą dėl išimties.

21. Informacijos saugos įgaliotinis raštu praneša išimties prašančiam Darbuotojui apie patvirtinimo pagrindimą arba atsisakymo paaiškinimą.

22. Jei prašymo patvirtinimas (teigiamas vizavimas) priklauso nuo specialių reikalavimų, kurie nėra užregistruoti prašymo formoje, išimties prašantis Darbuotojas privalo pasirašyti ir pateikti atnaujintą prašymo formą.

23. Visi išimčių prašymai turi būti dokumentuojami ir saugomi informacijos saugos įgaliotinio.

24. Jei nenurodyta kitaip, išimtys galioja vienerius metus.

VII SKRIUS
BAIGIAMOSIOS NUOSTATOS

25. Ši Procedūra tikrinama ir peržiūrima ne rečiau kaip vieną kartą per kalendorinius metus.

_____

Informacijos saugumo išimčių
valdymo procedūros
priedas

(Išimties prašymo formos pavyzdys)

Prašymo pateikėjas (vardas, pavardė):
Data:

Reikalavimas, kuriam prašoma išimties	
Priežastis, dėl kurios prašoma išimties	
Pasikeitusios situacijos, įgyvendinus išimtį, aprašymas	
Su reikalavimo nesilaikymu susijusios neatitikties rizikos įvertinimas	
Rizikos, susijusios su išimtimi, valdymo būdas	
Tikėtina išimties trukmė	
Papildoma informacija (jei reikia, pridėkite papildomą dokumentą)	

Patvirtinta	**Atmesta**	**Reikia daugiau informacijos**	**Informacijos saugos įgaliotinio parašas**	**Komisijos pirmininko parašas**	**Data**
Komentarai (įskaitant rizikos vertinimą)					

Valstybinės kainų ir energetikos kontrolės
komisijos Informacijos saugumo valdymo
sistemos aprašo
5 priedas

VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės kainų ir energetikos kontrolės komisijos (toliau – Komisija) veiklos tęstinumo valdymo plano paskirtis – įvertinti kritines situacijas, neutralizuoti veiklos sutrikdymą, apsaugoti veiklos procesus nuo padarinių, įvykus kritinėms situacijoms ir užtikrinti Komisijos veiklos atnaujinimą, tęstinumą bei informacinių išteklių saugumą tokių situacijų metu.

2. Procedūra taikoma visoms Komisijos veikloms ir informaciniams ištekliams, skirtiems toms veikloms vykdyti, įskaitant Komisijos valstybės tarnautojus, pareigūnus ir darbuotojus, dirbančius pagal darbo sutartis (toliau – Darbuotojai), veiklos procesus, darbo aplinką, infrastruktūrą.

3. Šiame Komisijos dokumente vartojamos sąvokos:

Informacijos saugumas – apima informacijos konfidencialumo, vientisumo ir pasiekiamumo išsaugojimą.

Informacinio ištekliaus savininkas – darbuotojas, atsakingas už informacinio ištekliaus priežiūrą ir informacijos saugumo reikalavimų nustatymą priskirtam informaciniam ištekliui.

Informacijos saugos įgaliotinis – Komisijos pirmininko įsakymu paskirtas Komisijos darbuotojas, atsakingas už informacijos saugumo valdymo Komisijoje įgyvendinimą ir palaikymą.

Kritinė situacija – informacijos saugumo incidentas, dėl kurio sutrinka ar gali sutrikti pagrindiniai Komisijos veiklos procesai.

II SKYRIUS
FUNKCIJOS IR ATSAKOMYBĖS

4. Už veiklos tęstinumo valdymą Komisijoje atsakingi:

4.1. Veiklos atkūrimo grupė;

4.2. Informacijos saugos įgaliotinis.

5. Veiklos atkūrimo grupė atsakinga už Komisijos veiklos tęstinumui kylančių grėsmių valdymo užtikrinimą, įvykus kritinei situacijai funkcijos, bei veiklos atkūrimo koordinavimą. Veiklos atkūrimo grupės funkcijos:

5.1. situacijos analizė ir sprendimų Komisijos veiklos tęstinumo valdymo klausimais priėmimas;

5.2. bendravimas su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;

5.3. bendravimas su susijusių kitų organizacijų veiklos tęstinumo valdymo grupėmis;

5.4. bendravimas su teisėsaugos ir kitomis institucijomis, institucijos darbuotojais ir kitomis interesų grupėmis;

5.5. paskirtų finansinių ir kitų išteklių, reikalingų Komisijos veiklai atkurti, įvykus kritinei situacijai, naudojimo kontrolė;

5.6. logistika (žmonių, daiktų, įrangos gabenimas ir jo organizavimas);

5.7. Komisijos veiklos atkūrimo priežiūra ir koordinavimas;

5.8. kitos Komisijos veiklos atkūrimo grupei pavestos funkcijos.

6. Informacijos saugos įgaliotinio funkcijos veiklos tęstinumo valdyme:

6.1. tobulina ir analizuoja veiklos tęstinumo valdymo procedūrą;

6.2. organizuoja veiklos tęstinumo valdymo bandymus ir protokoluoja (Veiklos tęstinumo valdymo testavimo protokolo forma pateikta priede) rezultatus;

6.3. teikia rizikos vertinimo rezultatus veiklos atkūrimo grupei, siekiant įvertinti ar į veiklos tęstinumo valdymą nereikia įtraukti papildomų scenarijų.

III SKYRIUS
VEIKLOS TĘSTINUMO VALDYMO TIKSLAI

7. Veiklos tęstinumo valdymas pagrįstas rizikos vertinimo rezultatais – atsižvelgiama į didžiausią riziką, kylančią informaciniams ištekliams, dėl kurios gali susidaryti kritinės situacijos.

8. Veiklos atkūrimo prioritetai yra šie:

8.1. Komisijos Darbuotojų sveikatos ir gyvybės apsauga;

8.2. informacinių technologijų veiklos atstatymas;

8.3. kiek galima greitesnis sutrikusios Komisijos veiklos atstatymas;

9. Kritinės situacijos, galinčios sutrikdyti Komisijos veiklą:

9.1. nepasiekiamos patalpos;

9.2. nepasiekiamas duomenų centras;

9.3. nepasiekiama techninė įranga;

9.4. nepasiekiami ar sugadinti duomenys;

9.5. nepasiekiami ryšiai;

9.6. nepasiekiami darbuotojai.

IV SKYRIUS
VEIKLOS TĘSTINUMO VALDYMAS

10. Visi Komisijos skyrių vedėjai ir informacinių išteklių savininkai turi būti supažindinti su veiklos tęstinumo valdymo procedūra. Skyrių vedėjai privalo supažindinti savo darbuotojus su jų pareigomis, sprendžiant kritines situacijas.

11. Iškilus kritinei situacijai Komisijos pirmininkas ar jo įgaliotas asmuo sudaro veiklos atkūrimo grupę, kurią sudaro:

11.1. Komisijos pirmininko paskirti skyrių vedėjai ir jų įgalioti asmenys;

11.2. informacijos saugos įgaliotinis;

11.3. finansininkas;

11.4. teisininkas;

11.5. veiklos procesų savininkai;

11.6. asmuo, atsakingas už viešuosius ryšius;

11.7. asmuo, atsakingas už fizinę saugą ir patalpų priežiūrą.

12. Ne rečiau kaip kartą per metus Informacijos saugos įgaliotinis inicijuoja Komisijos veiklos tęstinumo valdymo testavimus ir nustato testavimo apimtį, parenkant vieną, kelis ar visus kritinių situacijų scenarijus. Testavimai atliekami vienu iš numatytų būdu:

12.1. teorinio modeliavimo metodas;

12.2. dalinio testavimo metodas;

12.3. kritinės situacijos imitavimo metodas.

13. Testavimo rezultatai protokoluojami ir saugomi 3 metus.

14. Įvykus kritinei situacijai ir iškilus grėsmei, kad Komisija negalės vykdyti savo veiklų, pirmiausiai apie tai turi būti informuojamas Komisijos pirmininkas, jį pavaduojantis asmuo, veiklos atkūrimo grupės vadovas, Informacijos saugos įgaliotinis.

15. Komisijos pirmininkas, įvertinęs kritinės situacijos mastą ir nustatęs, kad Komisijos veikla gali būti sutrikdyta ilgiau nei 1 dienai, inicijuoja kritinės situacijos valdymo veiksmus, numatytus Komisijos veiklos tęstinumo valdymo plane. Veiklos tęstinumo valdymo plane numatyti kritinių situacijų, galinčių sutrikdyti Komisijos veiklą, scenarijai, atsakomieji veiksmai, atsakingi darbuotojai ir kiekvieno veiksmo atlikimo laikas.

V SKYRIUS
BENDRASIS VEIKLOS TĘSTINUMO PLANAS

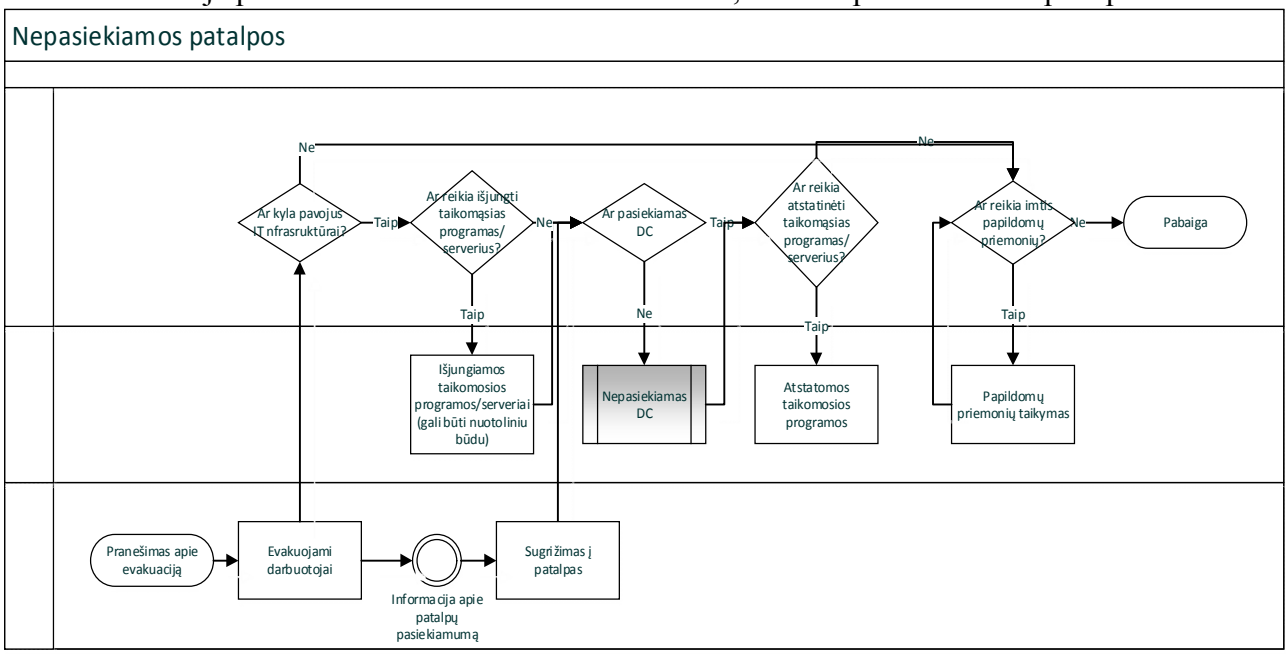
16. Žemiau aprašytos galimos kritinės situacijos ir veiksmai, kurie turi būti atlikti, siekiant užtikrinti veiklos tęstinumą.

16.1. Kritinė situacija 1: Nepasiekiamos patalpos

Kritinė situacija	**Atliekami veiksmai**	**Atsakingi darbuotojai**	**Veiksmų atlikimo laikas**
1. Nepasiekiamos patalpos (vykdoma evakuacija dėl gaisro, patalpų užpuolimo, pavojingų medžiagų patalpose, patalpų pažeidimo arba praradimo, stichinės nelaimės, oro sąlygų, avarijų, karo veiksmų)	1.1.Evakuojami darbuotojai ir atliekami kiti veiksmai pagal darbų saugos instrukcijas	Atsakingas už darbų saugą	
	1.2. Įvertinama, ar kyla pavojus IT infrastruktūrai. Jei ne, toliau vykdomi veiksmai, numatyti 1.9 punktą. Jei taip, toliau vykdomi veiksmai, numatyti 1.3 punktą.	Veiklos atkūrimo grupė	
	1.3. Įvertinama, ar reikia išjungti taikomąsias programas/serverius. Jei ne, toliau vykdomi veiksmai, numatyti 1.5 punktą. Jei taip, toliau vykdomi veiksmai, numatyti 1.4 punktą.	Veiklos atkūrimo grupė	
	1.4. Jei reikia, išjungiamos taikomosios programos/serveriai (gali būti nuotoliniu būdu vykdoma)	Veiklos atkūrimo grupė	
	1.5 Nustatoma, ar pasiekiamas duomenų centras. Jei ne, toliau vykdomi veiksmai, numatyti 1.6 punktą. Jei taip, toliau vykdomi veiksmai, numatyti 1.7 punktą.	Veiklos atkūrimo grupė	
	1.6. Vykdomi veiksmai, numatyti pagal 2 scenarijų.	Veiklos atkūrimo grupė	
	1.7. Priimamas sprendimas, ar reikia atstatinėti taikomųjų programų/serverių veiklą. Jei ne, toliau vykdomi veiksmai, numatyti 1.9 punktą. Jei taip, toliau vykdomi	Veiklos atkūrimo grupė	

Kritinė situacija	Atliekami veiksmai	Atsakingi darbuotojai	Veiksmų atlikimo laikas
	veiksmai, numatyti 1.8 punktą.		
	1.8. Atstatomos taikomosios programos/serveriai	Veiklos atkūrimo grupė	
	1.9. Įvertinama, ar reikia imtis papildomų priemonių. Jei ne, laikoma, kad veikla atkurta. Jei taip, toliau vykdomi veiksmai, numatyti 1.10 punktą.	Veiklos atkūrimo grupė	
	1.10. Taikomos papildomos priemonės	Veiklos atkūrimo grupė	
	1.11 Informuojami darbuotojai apie patalpų pasiekiamumą, kai gaunama informacija, kad patalpos tinkamos naudoti.	Veiklos atkūrimo grupė	

Žemiau schemoje pavaizduoti veiklos atkūrimo veiksmai, esant nepasiekiamoms patalpoms

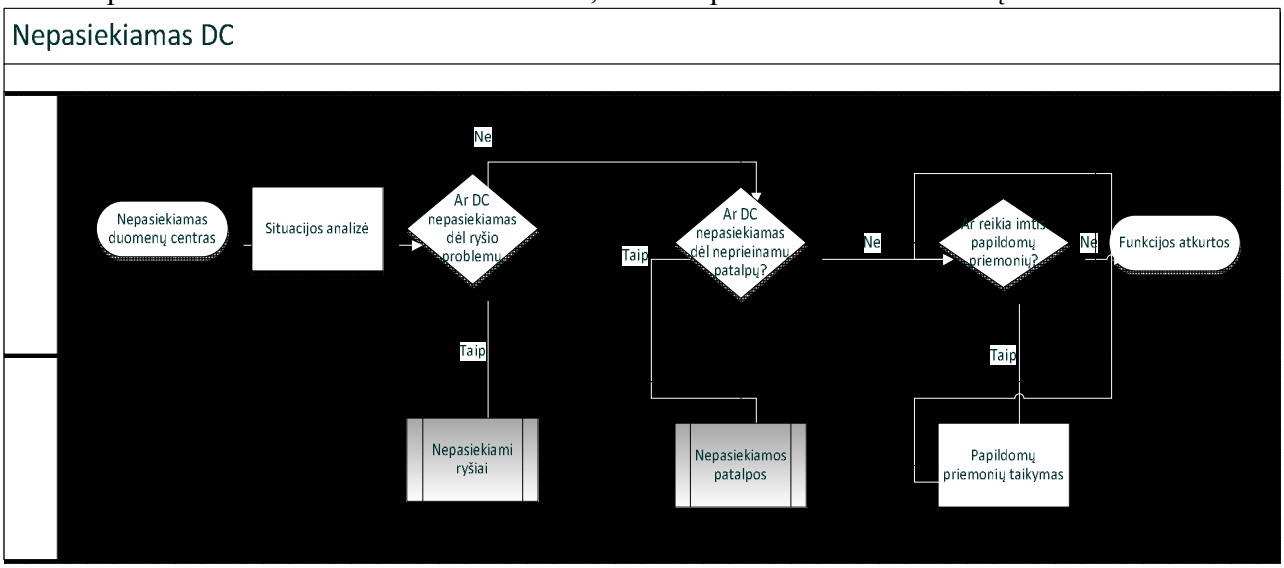


16.2. Kritinė situacija 2: Nepasiekiamas duomenų centras

Kritinė situacija	Atliekami veiksmai	Atsakingi darbuotojai	Veiksmų atlikimo laikas
2. Nepasiekiamas duomenų centras (dėl gaisro pastate ar	2.1. Nustatoma, kad nepasiekiamas duomenų centras	Situaciją pastebėjęs darbuotojas	
	2.2. Situacijos analizė	Veiklos atkūrimo grupė	

Kritinė situacija	Atliekami veiksmai	Atsakingi darbuotojai	Veiksmų atlikimo laikas
DC patalpose, dėl inžinerinių sistemų gedimo (rezervinės elektros maitinimo, kondicionavimo ir vėdinimo ir pan.)	2.3. Įvertinama, ar reikia imtis papildomų priemonių. Jei ne, toliau vykdomi veiksmai, numatyti 2.5 punktą. Jei taip, toliau vykdomi veiksmai, numatyti 2.4 punktą.	Veiklos atkūrimo grupė	
	2.4. Taikomos papildomos priemonės. Toliau vykdomi veiksmai, numatyti 2.3. punkte.	Veiklos atkūrimo grupė	
	2.5. Įvertinama, ar galima naudotis duomenų centru. Jei ne, toliau vykdomi veiksmai, numatyti 2.3 punktą. Jei taip, toliau vykdomi veiksmai, numatyti 2.6 punktą.	Veiklos atkūrimo grupė	
	2.6. Infrastruktūros atstatymas duomenų centre. Veikla atkurta.	Veiklos atkūrimo grupė	

Žemiau pavaizduota veiklos atkūrimo schema, esant nepasiekiamam duomenų centrui

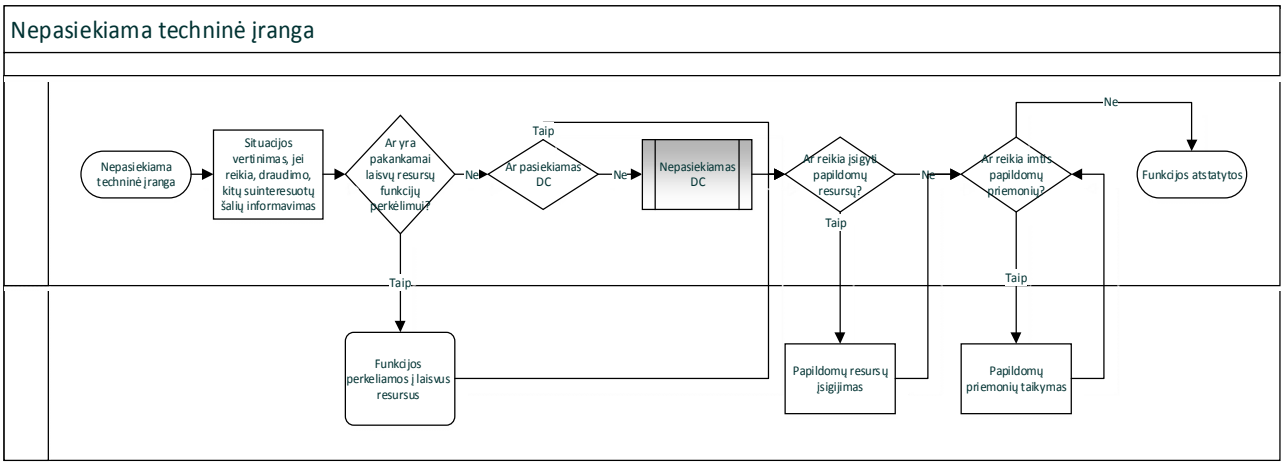


16.3. Kritinė situacija 3: Nepasiekiama techninė įranga

Kritinė situacija	Atliekami veiksmai	Atsakingi darbuotojai	Veiksmų atlikimo laikas
3. Nepasiekiama techninė įranga (dėl techninės įrangos gedimo, neturint rezervinės	3.1. Nustatoma, kad nepasiekiama techninė įranga.	Situaciją pastebėjęs darbuotojas	
	3.2. Situacijos vertinimas, jei reikia, draudimo įmonės, kitų suinteresuotų šalių informavimas	Veiklos atkūrimo grupė	

Kritinė situacija	Atliekami veiksmai	Atsakingi darbuotojai	Veiksmų atlikimo laikas
įrangos)	3.3 Nustatoma, ar yra pakankamai resursų funkcijų perkėlimui. Jei ne, toliau vykdomi veiksmai, numatyti 3.5 punktą. Jei taip, toliau vykdomi veiksmai, numatyti 3.4 punktą.	Veiklos atkūrimo grupė	
	3.4. Funkcijos perkeliamos į laisvus resursus. Toliau vykdomi veiksmai, numatyti 3.5. punkte.	Veiklos atkūrimo grupė	
	3.5. Nustatoma, ar pasiekiamas duomenų centras. Jei ne, toliau vykdomi veiksmai, numatyti pagal 2 scenarijų. Jei taip, toliau vykdomi veiksmai, numatyti 3.6 punktą.	Veiklos atkūrimo grupė	
	3.6. Nustatoma, ar reikia įsigyti papildomų resursų. Jei ne, toliau vykdomi veiksmai, numatyti 3.8 punktą. Jei taip, toliau vykdomi veiksmai, numatyti 3.7 punktą.	Veiklos atkūrimo grupė	
	3.7. Papildomų resursų įsigijimas.	Veiklos atkūrimo grupė	
	3.8. Nustatoma, ar reikia imtis papildomų priemonių. Jei ne, toliau vykdomi veiksmai, numatyti 3.10 punktą. Jei taip, toliau vykdomi veiksmai, numatyti 3.9 punktą.	Veiklos atkūrimo grupė	
	3.9. Papildomų priemonių taikymas. Toliau vykdomi veiksmai, numatyti 3.8. punkte.	Veiklos atkūrimo grupė	
	3.10. Priimamas sprendimas, kad funkcijos atstatytos	Veiklos atkūrimo grupė	

Žemiau pavaizduota veiklos atkūrimo schema, esant nepasiekiamai techninei įrangai.

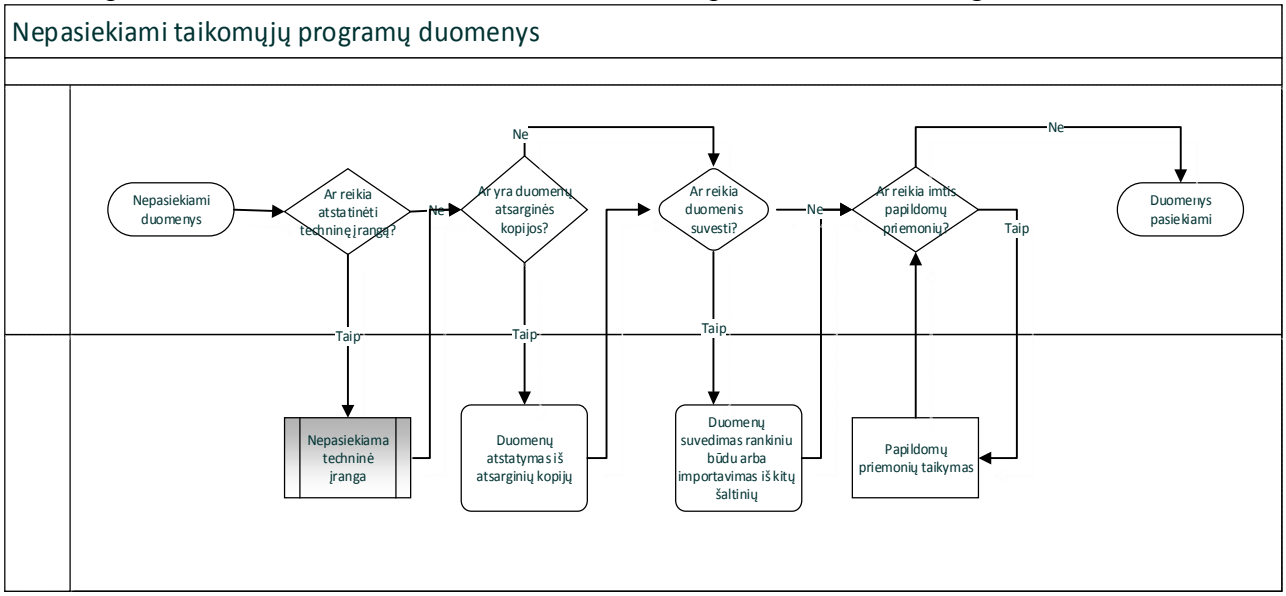


16.4. Kritinė situacija 4: Nepasiekiami ar sugadinti duomenys

Kritinė situacija	**Atliekami veiksmai**	**Atsakingi darbuotojai**	**Veiksmų atlikimo laikas**
4. Nepasiekiami ar sugadinti duomenys (kai pažeistas duomenų bazės integralumas, sugadinti duomenys atsarginėse kopijose, dėl kenksmingos programinės įrangos, dėl elektromagnetinio poveikio)	4.1. Nustatoma, kad duomenys nepasiekiami.	Situaciją pastebėjęs darbuotojas	
	4.2. Įvertinama, ar reikia atstatinėti techninę įrangą. Jei ne, toliau vykdomi veiksmai, numatyti 4.3 punktą. Jei taip, toliau vykdomi veiksmai pagal 3 scenarijų.	Veiklos atkūrimo grupė	
	4.3. Nustatoma, ar yra duomenų atsarginės kopijos. Jei ne, toliau vykdomi veiksmai, numatyti 4.5 punktą. Jei taip, toliau vykdomi veiksmai, numatyti 4.4 punktą.	Veiklos atkūrimo grupė	
	4.4. Duomenų atstatymas iš atsarginių kopijų.	Veiklos atkūrimo grupė	
	4.5. Nustatoma, ar reikia duomenis suvesti. Jei ne, toliau vykdomi veiksmai, numatyti 4.7 punktą. Jei taip, toliau vykdomi veiksmai, numatyti 4.6 punktą.	Veiklos atkūrimo grupė	
	4.6. Duomenų suvedimas rankiniu būdu arba importavimas iš kitų šaltinių	Veiklos atkūrimo grupė	
	4.7. Nustatoma, ar reikia imtis papildomų priemonių Jei ne, toliau vykdomi veiksmai, numatyti 4.8 punktą.	Veiklos atkūrimo grupė	

Kritinė situacija	Atliekami veiksmai	Atsakingi darbuotojai	Veiksmų atlikimo laikas
	Jei taip, toliau vykdomi veiksmai, numatyti 4.8 punktą.		
	4.8. Papildomų priemonių taikymas	Veiklos atkūrimo grupė	
	4.9. Duomenys pasiekiami	Veiklos atkūrimo grupė	

Žemiau pavaizduota veiklos atkūrimo schema, esant nepasiekiamiems ar sugadintiems duomenims

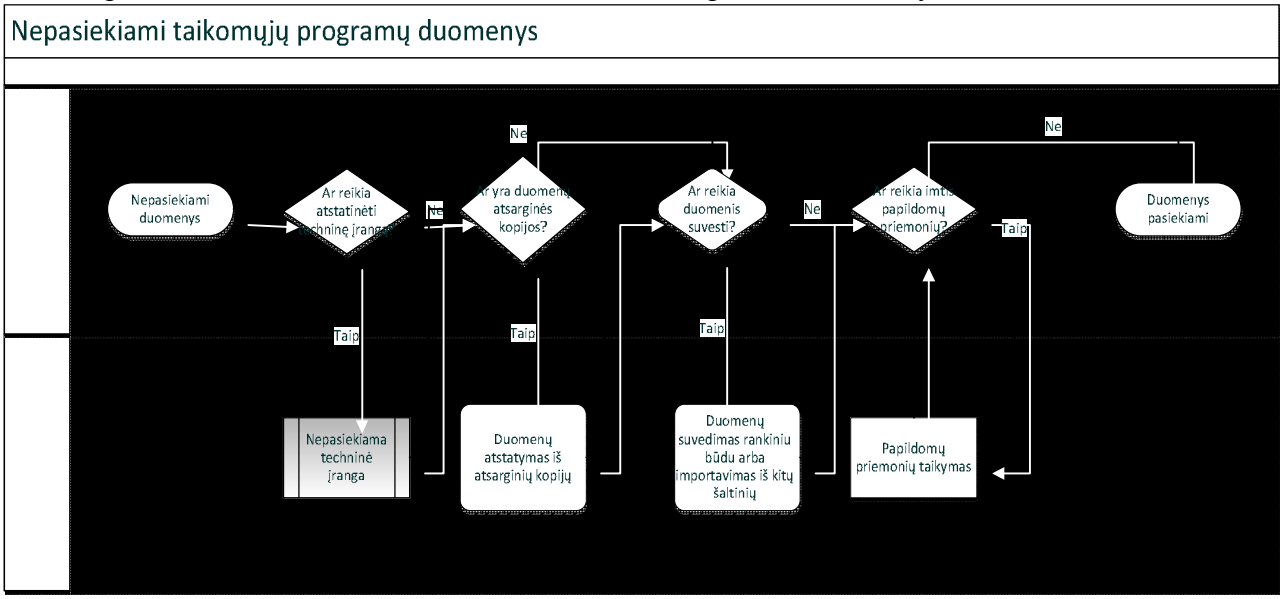


16.5. Kritinė situacija 5: Nepasiekiami ryšiai

Kritinė situacija	Atliekami veiksmai	Atsakingi darbuotojai	Veiksmų atlikimo laikas
5. Nepasiekiami ryšiai (dėl dingusio ryšio su paslaugų tiekėju (interneto), optinių kabelių nutrūkimas, dėl kibernetinių atakų)	5.1 Nustatoma, kad nepasiekiami ryšiai.	Situaciją pastebėjęs darbuotojas	
	5.2. Situacijos analizė ir naudotojų informavimas apie sutrikimus	Veiklos atkūrimo grupė	
	5.3. Nustatoma, ar reikia organizuoti alternatyvius ryšius. Jei ne, toliau vykdomi veiksmai, numatyti 5.5 punktą. Jei taip, toliau vykdomi veiksmai, numatyti 5.4 punktą.	Veiklos atkūrimo grupė	
	5.4. Alternatyvių ryšio priemonių organizavimas	Veiklos atkūrimo grupė	
	5.5. Nustatoma, ar reikia imtis papildomų priemonių. Jei ne, toliau vykdomi veiksmai, numatyti 5.7 punktą.	Veiklos atkūrimo grupė	

Kritinė situacija	Atliekami veiksmai	Atsakingi darbuotojai	Veiksmų atlikimo laikas
	Jei taip, toliau vykdomi veiksmai, numatyti 5.6 punktą.		
	5.6. Papildomų priemonių taikymas	Veiklos atkūrimo grupė	
	5.7. Ryšiai atstatyti	Veiklos atkūrimo grupė	

Žemiau pavaizduota veiklos atkūrimo schema, esant nepasiekiamiems ryšiams.

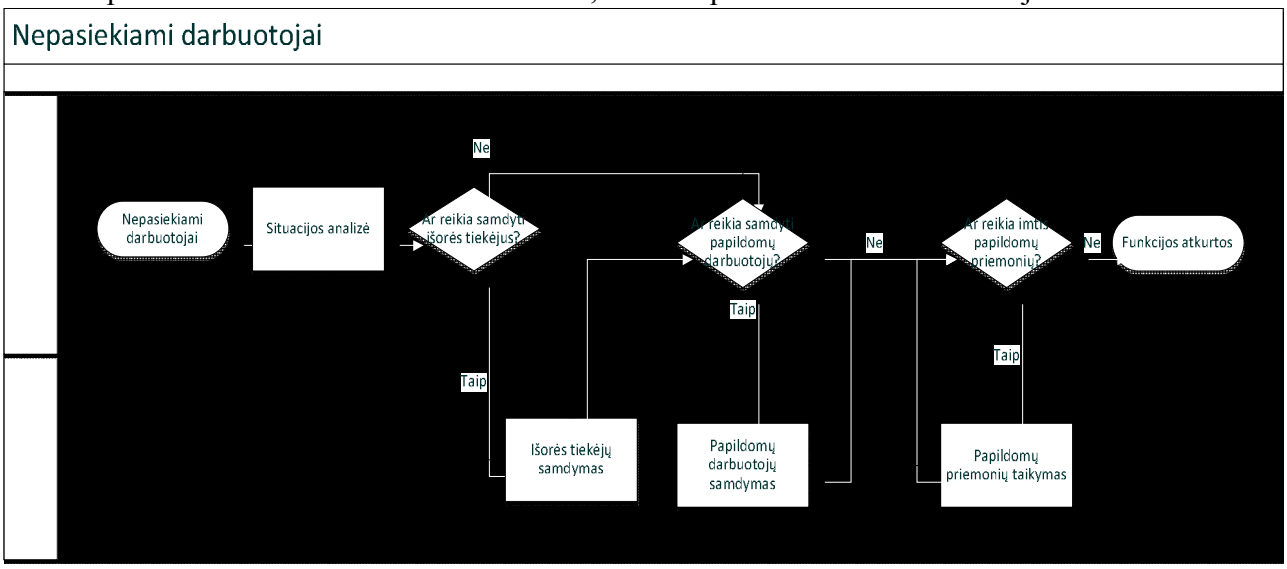


16.6. Kritinė situacija 6: Nepasiekiami darbuotojai.

Kritinė situacija	Atliekami veiksmai	Atsakingi darbuotojai	Veiksmų atlikimo laikas
6. Nepasiekiami darbuotojai (kai negali atvykti į darbą daugiau nei penktadalis darbuotojų dėl oro sąlygų, stichinių nelaimių, avarijų, epidemijų, mobilizacijos, cheminės atakos, karo veiksmų ir pan.)	6.1. Nustatoma, kad nepasiekiami darbuotojai	Veiklos atkūrimo grupė	
	6.2. Situacijos analizė	Veiklos atkūrimo grupė	
	6.3. Nustatoma, ar reikia samdyti išorinius tiekėjus. Jei ne, toliau vykdomi veiksmai, numatyti 6.5 punktą. Jei taip, toliau vykdomi veiksmai, numatyti 6.4 punktą.	Veiklos atkūrimo grupė	
	6.4. Išorinių tiekėjų samdymas	Veiklos atkūrimo grupė	
	6.5. Nustatoma, ar reikia samdyti papildomų darbuotojų. Jei ne, toliau vykdomi veiksmai, numatyti 6.7 punktą. Jei taip, toliau vykdomi	Veiklos atkūrimo grupė	

Kritinė situacija	Atliekami veiksmai	Atsakingi darbuotojai	Veiksmų atlikimo laikas
	veiksmai, numatyti 6.6 punktą.		
	6.6. Papildomų darbuotojų samdymas	Veiklos atkūrimo grupė	
	6.7. Nustatoma, ar reikia imtis papildomų priemonių. Jei ne, toliau vykdomi veiksmai, numatyti 6.9 punktą. Jei taip, toliau vykdomi veiksmai, numatyti 6.8 punktą.	Veiklos atkūrimo grupė	
	6.8. Papildomų priemonių taikymas	Veiklos atkūrimo grupė	
	6.9. Laikoma, kad funkcijos atkurtos	Veiklos atkūrimo grupė	

Žemiau pavaizduota veiklos atkūrimo schema, esant nepasiekiamiems darbuotojams.



VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

17. Veiklos tęstinumo valdymo plano veiksmingumas tikrinamas kiekvienais metais. Nustatytą dieną imituojamos kritinės situacijos, jų metu atsakingi pasekmių likvidavimo vykdytojai atlieka kritinės situacijos veiksmus.

18. Informacijos saugos įgaliotinis atsakingas už Veiklos tęstinumo valdymo plano veiksmingumo išbandymo metu pastebėtų trūkumų ataskaitos parengimą ir teikimą peržiūrai vadovybės vertinamosios analizės posėdžiui.

19. Veiklos tęstinumo valdymo plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami remiantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

_____

Veiklos tęstinumo valdymo plano
priedas

(Veiklos tęstinumo valdymo testavimo protokolo forma)

Testavimui vadovaujantis asmuo	*Vardas Pavardė*
Testavime dalyvaujantys asmenys	*Vardas Pavardė, pareigos*
Darbotvarkė	*PVZ.:* *1. Veiklos tęstinumo valdymo procedūros peržiūra* *2. Veiklos tęstinumo valdymo testavimas*
Testuotos situacijos	*Įrašyti tekstą.*
Testavimo rezultatai ir priimti sprendimai	*Įrašyti tekstą.*

Valstybinės kainų ir energetikos kontrolės
komisijos Informacijos saugumo valdymo
sistemos aprašo
6 priedas

INFORMACIJOS APSAUGOS PRIEMONIŲ VEIKSMINGUMO MATAVIMO PROCESAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės kainų ir energetikos kontrolės komisijos informacijos apsaugos priemonių veiksmingumo matavimo procesas reglamentuoja informacijos apsaugos priemonių veiksmingumo matavimo tvarką Valstybinėje kainų ir energetikos kontrolės komisijoje (toliau – Komisija), siekiant užtikrinti Komisijos disponuojamos informacijos saugumą ir atitikti informacijos saugumui keliamus reikalavimus. Informacijos apsaugos priemonių veiksmingumo matavimo tvarka apima informacijos apsaugos priemonių veiksmingumo matavimo būdus, veiklas, atsakomybes veiklų matavimo tvarkose, veiksmingumo matavimo kriterijus, rezultatų vertinimą.

2. Komisijos informacijos apsaugos priemonių veiksmingumo matavimo procesas yra privalomas visiems Komisijos valstybės tarnautojams, pareigūnams ir darbuotojams, dirbantiems pagal darbo sutartis (toliau – Darbuotojai).

3. Šiame Komisijos informacijos apsaugos priemonių veiksmingumo matavimo procese vartojamos sąvokos:

Informacijos saugumas – apima informacijos konfidencialumo, vientisumo ir pasiekiamumo išsaugojimą.

Informacijos saugos įgaliotinis – Komisijos pirmininko įsakymu paskirtas Komisijos darbuotojas, atsakingas už informacijos saugumo valdymo Komisijoje įgyvendinimą ir palaikymą.

ISVS – Informacijos saugumo valdymo sistema.

Vadovybės vertinamoji ISVS analizė – tai vadovybės atliekamas visapusiškas veiklos nagrinėjimas, nustatantis ISVS efektyvumą, atitiktį reikalavimams bei numatantis galimus ISVS tobulinimo veiksmus.

II SKYRIUS
FUNKCIJOS IR ATSAKOMYBĖS

4. Už informacijos apsaugos priemonių veiksmingumo matavimo valdymą Komisijoje atsakingi šie darbuotojai:

4.1. Informacijos saugos įgaliotinis:

4.1.1. renka informacijos saugumo veiksmingumo nustatymo duomenis nustatytu periodiškumu ir būdais;

4.1.2. analizuoja veiksmingumo nustatymo duomenis ir juos vertina pagal nustatytus priimtinumo kriterijus;

4.1.3. imasi atsakomųjų veiksmų pagal nustatytus sprendimo priėmimo kriterijus;

4.1.4. išsiaiškina ir pašalina priežastis, numato korekcinius veiksmus, jei veiksmingumo rezultatai nepriimtini;

4.1.5. registruoja ir sprendžia informacijos saugumo incidentus, numato priemones incidento priežastims pašalinti tuo atveju, kai veiksmingumo rezultatai nustatomi kaip pavojingi;

4.1.6. veiksmingumo matavimo žurnale (1 priedas) pildo veiksmingumo nustatymo duomenis ir jų vertinimo rezultatus;

4.1.7. ne rečiau kaip kartą per metus pateikia apibendrinančius veiksmingumo matavimo rezultatus vadovybės vertinamajai analizei (pateikia užpildytą veiksmingumo matavimo žurnalą su vertinimo siūlymais (priimtina, nepriimtina, pavojinga), kokių atsakomųjų veiksmų buvo imtasi (jei buvo) bei, jei reikia, siūlymus, kaip pašalinti nepriimtino ar pavojingo veiksmingumo priežastis).

4.2. Komisijos darbuotojai, susiję ar esantys atsakingi su veiksmingumo matavimo objektus teikia Informacijos saugos įgaliotiniui duomenis, reikalingus atlikti veiksmingumo matavimą.

III SKYRIUS
VEIKSMINGUMO MATAVIMO APIMTIS

5. Informacijos apsaugos priemonių veiksmingumas vertinamas, matuojant:

5.1. informacijos saugumo dokumentų aktualumą ir peržiūrą – analizuojama ir matuojama ar informacijos saugumo dokumentai periodiškai peržiūrimi ir yra aktualūs;

5.2. mobiliųjų įrenginių naudojimą – analizuojama ir matuojama, ar mobilieji įrenginiai naudojami pagal jiems keliamus reikalavimus;

5.3. prieigos valdymą – analizuojamas ir matuojamas prieigos valdymas bei naudojamų slaptažodžių kokybė;

5.4. informacijos apsaugos valdymo priemonių įgyvendinimo efektyvumą – analizuojama ir matuojama informacijos apsaugos valdymo priemonių įgyvendinimo trukmė pagal rizikos tvarkymo planą;

5.5. informacijos saugumo incidentų valdymo efektyvumą - analizuojamas ir matuojamas visų informacijos saugumo incidentų skaičiaus pokytis, lyginant su praėjusiu laikotarpiu, taip pat I kategorijos informacijos saugumo incidentų skaičiaus pokytis, lyginant su praėjusiu laikotarpiu;

5.6. informacijos saugumo valdymo sistemos neatitikčių šalinimo efektyvumą - analizuojamas ir matuojamas nustatytų ir pašalintų informacijos saugumo valdymo sistemos neatitikčių skaičius;

5.7. Darbuotojų mokymų ir sąmoningumo informacijos saugumo srityje valdymo efektyvumą - analizuojamas ir matuojamas pagal mokymų planą apmokytų informacijos saugumo srityje Komisijos valstybės tarnautojų, pareigūnų ir darbuotojų, dirbančių pagal darbo sutartis skaičius;

5.8. saugumo, susijusio su išoriniais paslaugų tiekėjais, valdymo efektyvumą - analizuojamas ir matuojamas išorinių paslaugų tiekėjų sutarčių, kuriose yra ir kuriose nėra reikalavimų, susijusių su informacijos saugumu, skaičius;

5.9. veiklos tęstinumo valdymo efektyvumą – analizuojami ir matuojami veiklos tęstinumo valdymo planų bandymų rezultatai bei šių planų bandymų trukmė.

6. Veiksmingumo matavimo apimtis peržiūrima vadovybės vertinamosios analizės metu. Informacijos saugos įgaliotinis teikia pasiūlymus dėl veiksmingumo matavimo apimties, atsižvelgdamas į nustatytus informacijos saugumo tikslus, ankstesnius veiksmingumo matavimo rezultatus, informacijos saugumo rizikos vertinimo rezultatus.

IV SKYRIUS
VEIKSMINGUMO MATAVIMO BŪDAI IR VERTINIMO KRITERIJAI

7. Pagal žemiau nustatytus kriterijus veiksmingumo matavimo rezultatai gali būti vertinami taip:

7.1. priimtina – veiksmingumo matavimo rezultatai yra tinkami, nereikia imtis papildomų priemonių;

7.2. nepriimtina – veiksmingumo matavimo rezultatai nepriimtini, reikia imtis papildomų veiksmų: registruoti neatitiktį, atlikti korekcinius veiksmus, stebėti korekcinių veiksmų vykdymą;

7.3. pavojinga – taip įvertinti veiksmingumo matavimo rezultatai rodo, kad yra ženklus nukrypimas nuo norimo rezultato ir situacija kelia grėsmę informacijos saugumui, todėl turi būti registruojamas informacijos saugumo incidentas, jam priskiriama kategorija, nustatomos priežastys, paskiriamas atsakingas asmuo ir vykdomi veiksmai, kurie numatyti Informacijos saugumo incidentų valdymo tvarkos apraše.

8. **Informacijos saugumo dokumentų aktualumas ir peržiūra.**

8.1. Informacijos saugos dokumentų peržiūros matavimo tikslas – užtikrinti, kad informacijos saugumo valdymui būtų naudojama aktuali dokumentacija, kad ji būtų nuolat peržiūrima ir

atnaujinama. Informacijos saugos įgaliotinis kartą per metus surenka duomenis, vadovaudamasis 2 priede pateiktu klausimynu ir įvertina juos pagal šiuos kriterijus:

8.1.1. jei informacijos saugumą reglamentuojantys visi dokumentai peržiūrėti, yra visi reikalingi įrašai – priimtina;

8.1.2. jei dalis ar visi dokumentai neperžiūrėti, naudojamos neaktualios jų versijos – nepriimtina.

9. **Mobiliųjų įrenginių naudojimas.**

9.1. Mobiliųjų įrenginių naudojimo veiksmingumo matavimo tikslas – užtikrinti, kad mobilieji įrenginiai atitinka jiems keliamus saugumo reikalavimus. Informacijos saugos įgaliotinis kartą per metus surenka duomenis, vadovaudamasis 3 priede pateiktu klausimynu ir įvertina juos pagal šiuos kriterijus:

9.1.1. jei iš patikrintų mobiliųjų įrenginių visi atitinka jiems keliamus informacijos saugumo reikalavimus – priimtina;

9.1.2. jei iš patikrintų mobiliųjų įrenginių iki 20% įrenginių neatitinka jiems keliamų informacijos saugumo reikalavimų – nepriimtina;

9.1.3. jei iš patikrintų mobiliųjų įrenginių daugiau kaip 20% neatitinka jiems keliamų informacijos saugumo reikalavimų – pavojinga.

10. **Prieigos valdymas**.

10.1. Tikslas – tinkamai valdyti prieigą ir užtikrinti Komisijos naudotojų slaptažodžių kokybę. Informacijos saugos įgaliotinis karta į metus surenka duomenis, vadovaujantis 4 priede pateiktu klausimynu, ir įvertina juos pagal šiuos kriterijus:

10.1.1. jei atlikus prieigos teisių peržiūrą nustatoma, kad visi darbuotojai turi prieigą prie tų finansinių išteklių, kurie jiems reikalingi darbo užduotims atlikti, nėra suteiktų perteklinių prieigos teisių – priimtina;

10.1.2. jei atlikus prieigos teisių peržiūrą nustatoma, kad iki 20% darbuotojų turi perteklines prieigos teises arba yra sąrašuose, nors jau nebedirba Komisijoje – nepriimtina;

10.1.3. jei atlikus prieigos teisių peržiūrą nustatoma, kad daugiau nei 20% darbuotojų turi perteklines prieigos teises arba yra sąrašuose, nors jau nebedirba Komisijoje – pavojinga;

10.1.4. jei atitinkančių nustatytus reikalavimus slaptažodžių dalis yra ne mažesnė nei 80 % - priimtina;

10.1.5. jei atitinkančių nustatytus reikalavimus slaptažodžių dalis yra nuo 60 iki 80 % - nepriimtina;

10.1.6. jei atitinkančių nustatytus reikalavimus slaptažodžių dalis yra mažesnė nei 60% - pavojinga, būtina imtis neatidėliotinų veiksmų – registruoti ir spręsti informacijos saugumo incidentą, nustatyti priežastis, numatyti incidento priežasčių pašalinimo priemones.

11. **Informacijos apsaugos valdymo priemonių įgyvendinimo efektyvumas.**

11.1. Informacijos apsaugos valdymo priemonių įgyvendinimo efektyvumo matavimo tikslas – stebėti ir kontroliuoti informacijos apsaugos valdymo priemonių įgyvendinimo efektyvumą, užtikrinti, kad informacijos saugumas įgyvendinamas ir vykdomas vadovaujantis Komisijos informacijos saugumo politika ir procedūromis. Informacijos saugos įgaliotinis kartą į metus surenka duomenis, remdamasis ataskaitomis apie informacijos apsaugos valdymo priemonių diegimą pagal patvirtintą rizikos valdymo planą bei vadovaudamasis 5 priede pateiktu klausimynu, ir įvertina juos pagal šiuos kriterijus:

11.1.1. jei nesėkmingai įdiegtų informacijos apsaugos valdymo priemonių per ataskaitinį laikotarpį nėra – priimtina. Nesėkmingai įdiegtomis laikomos informacijos saugumo valdymo priemonės, kurios yra neįdiegtos laiku (pagal terminą, nustatyta rizikos valdymo plane) arba įdiegtos daugiau kaip 20% viršijant planuotą reikalingų išteklių kiekį arba akivaizdžiai nedavė laukiamos naudos;

11.1.2. jei yra bent viena nesėkmingai įdiegta informacijos apsaugos valdymo priemonė bendrame planuotų valdymo priemonių kiekyje – nepriimtina;

11.1.3. jei nesėkmingai įdiegtų informacijos saugumo valdymo priemonių dalis bendrame planuotų priemonių kiekyje daugiau kaip 20% - pavojinga.

12. **Informacijos saugumo incidentų valdymo efektyvumas.**

12.1. Informacijos saugumo incidentų valdymo efektyvumo matavimo tikslas – stebėti ir kontroliuoti informacijos saugumo incidentų sprendimo efektyvumą, mažinti veiklos riziką. Informacijos saugos įgaliotinis kartą per mėnesį surenka duomenis, remdamasis informacijos saugumo incidentų žurnalo įrašais bei vadovaudamasis 6 priede pateiktu klausimynu, ir vertina juos pagal šiuos kriterijus:

12.1.1. jei informacijos saugumo incidentų kiekio pokytis, palyginus su praėjusiu ataskaitiniu laikotarpiu, neviršija 50%. – priimtina;

12.1.2. jei informacijos saugumo incidentų kiekio pokytis, palyginus su praėjusiu ataskaitiniu laikotarpiu, yra nuo 50 iki 100%. – nepriimtina;

12.1.3. jei informacijos saugumo incidentų kiekio pokytis, palyginus su praėjusiu ataskaitiniu laikotarpiu, yra daugiau kaip 100% – pavojinga;

12.1.4. jei I kategorijos incidentų dalis visų nustatytų per ataskaitinį laikotarpį incidentų kiekyje neviršija 20% - priimtina;

12.1.5. jei I kategorijos incidentų dalis visų nustatytų per ataskaitinį laikotarpį incidentų kiekyje yra nuo 20 iki 50% – nepriimtina;

12.1.6. jei I kategorijos incidentų dalis visų nustatytų per ataskaitinį laikotarpį incidentų kiekyje yra daugiau kaip 50% – pavojinga.

13. **Informacijos saugumo valdymo sistemos neatitikčių šalinimo efektyvumas.**

13.1. Informacijos saugumo valdymo sistemos neatitikčių šalinimo efektyvumo matavimo tikslas – stebėti ir kontroliuoti informacijos saugumo valdymo sistemos neatitikčių šalinimo efektyvumą. Informacijos saugos įgaliotinis kartą per metus surenka duomenis, remdamasis vidaus auditų rezultatais bei neatitikčių šalinimo planais ir vadovaudamasis 7 priede pateiktu klausimynu, ir įvertina juos pagal šiuos kriterijus:

13.1.1. jei nepašalintų ar nesėkmingai pašalintų neatitikčių per ataskaitinį laikotarpį nėra – priimtina. Nesėkmingai pašalintomis laikomos neatitiktys, kurios nepašalintos laiku (pagal neatitikčių šalinimo planą) arba žymiai (daugiau kaip 20 %) viršijant numatytus neatitikties šalinimo išteklius;

13.1.2. jei nepašalintų ar nesėkmingai pašalintų neatitikčių dalis bendrame, su informacijos saugumo valdymo sistema susijusių, nustatytų neatitikčių kiekyje yra iki 20 % – nepriimtina;

13.1.3. jei nepašalintų ar nesėkmingai pašalintų neatitikčių dalis bendrame, su informacijos saugumo valdymo sistema susijusių, nustatytų neatitikčių kiekyje yra daugiau kaip 20 % – pavojinga.

14. **Darbuotojų mokymų ir sąmoningumo informacijos saugumo srityje valdymo efektyvumas.**

14.1. Darbuotojų mokymų ir sąmoningumo informacijos saugumo srityje valdymo efektyvumo tikslas – stebėti ir kontroliuoti darbuotojų kvalifikaciją informacijos saugumo srityje. Informacijos saugos įgaliotinis kartą į metus surenka duomenis, remiantis mokymų planu (-ais) ir vadovaujantis 8 priede pateiktu klausimynu, ir įvertina juos pagal šiuos kriterijus:

14.1.1. jei apmokytų pagal planą darbuotojų dalis yra daugiau nei 80% – priimtina;

14.1.2. jei apmokytų pagal planą darbuotojų dalis yra nuo 60 iki 80% – nepriimtina;

14.1.3. jei apmokytų pagal planą darbuotojų dalis yra mažesnė nei 60% – pavojinga.

15. **Saugumo, susijusio su išoriniais paslaugų tiekėjais, turinčiais prieigą, prie Komisijos informacinių išteklių, valdymo efektyvumas.**

15.1. Saugumo, susijusio su išoriniais paslaugų tiekėjais, valdymo efektyvumo matavimo tikslas – užtikrinti išorinių paslaugų tiekėjų įsipareigojimus saugoti informaciją. Informacijos saugos įgaliotinis kartą per metus surenka duomenis, vadovaudamasis 9 priede pateiktu klausimynu, ir įvertina juos pagal šiuos kriterijus:

15.1.1. jei nepasirašytų sutarčių, kuriose nenumatyti informacijos saugumo reikalavimai nėra – priimtina;

15.1.2. jei yra bent viena sutartis, kurioje nenumatyti informacijos saugumo reikalavimai – nepriimtina;

15.1.3. jei sutarčių, kuriose nenumatyti informacijos saugumo reikalavimai, yra daugiau nei 20% - pavojinga.

16. **Veiklos tęstinumo valdymo efektyvumas.**

16.1. Veiklos tęstinumo valdymo efektyvumo matavimo tikslas - stebėti ir kontroliuoti veiklos tęstinumo valdymo efektyvumą. Efektyvumas vertinamas pagal Komisijos veiklos tęstinumo valdymo plano bandymų rezultatus ir trukmę. Informacijos saugos įgaliotinis kartą per metus surenka duomenis, remdamasis Komisijos veiklos tęstinumo valdymo planų bandymų ataskaitomis bei vadovaudamasis 10 priede pateiktu klausimynu, ir įvertina juos pagal šiuos kriterijus:

16.1.1. jei visi Komisijos veiklos tęstinumo valdymo planų bandymai buvo sėkmingi ir neviršijo plane nustatytos atkūrimo trukmės, vertinama kaip priimtina;

16.1.2. jei bent vienas Komisijos veiklos tęstinumo valdymo plano bandymas buvo nesėkmingas arba viršijo nustatytą pagal planą atkūrimo trukmę iki 50%, vertinama kaip nepriimtina;

16.1.3. jei visi Komisijos veiklos tęstinumo valdymo plano bandymai buvo nesėkmingi arba išmatuota veiklos atkūrimo trukmė viršija nustatytą pagal planą daugiau kaip 50%, vertinama kaip pavojinga.

V SKYRIUS
VEIKSMINGUMO DIDINIMO BŪDAI

17. Į nepriimtinus ir pavojingus matavimo rezultatus Informacijos saugos įgaliotinis turi reaguoti per protingą laiką, išsamiai išanalizuoti priežastis ir jas pašalinti, registruoti informacijos saugumo incidentą, kai veiksmingumo vertinimas yra pavojingas. Laiku sprendžiami nepriimtini ir pavojingi vertinimai užkerta kelią tokių rezultatų pasikartojimui ateityje, leidžia pamatyti silpnas vietas ir gerinimo bei tobulinimo galimybes. Informacijos saugos įgaliotinis pateikia veiksmingumo matavimo rezultatus vadovybės vertinamajai analizei, kurios metu aptariami veiksmingumo matavimo rezultatai, veiksmingumo didinimo būdai (esant poreikiui) ir tobulinimo galimybės, peržiūrima veiksmingumo matavimo apimtis ir vertinimo kriterijai. Vadovybės vertinamosios analizės metu gali būti priimamas sprendimas taikyti vieną ar kelis veiksmingumo didinimo būdus:

17.1. keisti naudojamas, diegti naujas ar taikyti papildomas informacijos apsaugos valdymo priemones;

17.2. keisti procesą, procedūrą ar priemonę, kurios veiksmingumą siekiama didinti;

17.3. taikyti kitas priemones, atsižvelgiant į tai, kokios buvo nustatytos nepriimtino ar pavojingo veiksmingumo priežastys.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

18. Informacijos saugos įgaliotinis periodiškai peržiūri procesą ir inicijuoja pakeitimus šiais atvejais:

18.1. atsižvelgiant į vadovybės vertinamosios analizės posėdžio metu pateiktas pastabas ir pasiūlymus;

18.2. pastebėjęs, kad tam tikros proceso nuostatos neleidžia efektyviai vykdyti informacijos saugumo reikalavimų ir informacijos saugumo veiksmingumo nustatymo;

18.3. pasikeitus veiklos ir (ar) informacijos saugumo tikslams;

18.4. pasikeitus teisės aktų, reglamentuojančių informacijos saugumą, reikalavimams ar sutartiniams informacijos saugumo įsipareigojimams.

_____

Informacijos apsaugos priemonių
veiksmingumo matavimo proceso
1 priedas

(Informacijos apsaugos priemonių veiksmingumo matavimo žurnalo forma)

Parametras	**Matavimo periodiškumas ir data**
Informacijos saugumo dokumentų aktualumas ir peržiūra	**Kartą per metus, data**
Peržiūrėti dokumentai	
Neperžiūrėti dokumentai	
Mobiliųjų įrenginių naudojimas	**Kartą per metus, data**
Tikrinamų įrenginių skaičius	
Atitinkančių informacijos saugumo reikalavimus įrenginių skaičius	
Atitinkančių informacijos saugumo reikalavimus įrenginių procentinė dalis	
Neatitinkančių informacijos saugumo reikalavimus įrenginių skaičius	
Neatitinkančių informacijos saugumo reikalavimus įrenginių procentinė dalis	
Priimtinumas	
Prieigos valdymas	**Kartą per metus, data**
Darbuotojų, atitinkančių prieigos reikalavimus, skaičius	
Darbuotojų, atitinkančių prieigos reikalavimus, procentinė dalis	
Darbuotojų, neatitinkančių prieigos reikalavimus, skaičius	
Darbuotojų, neatitinkančių prieigos reikalavimus, procentinė dalis	
Priimtinumas	
Nustatytų slaptažodžių skaičius	
Slaptažodžių, kurie atitinka nustatytus reikalavimus, skaičius	
Slaptažodžių, kurie neatitinka nustatytų reikalavimų, skaičius	
Slaptažodžių, kurie neatitinka nustatytų reikalavimų, dalis (%)	
Priimtinumas	
Informacijos saugumo valdymo priemonių įgyvendinimas	**Kartą per metus, data**
Planuotų įdiegti per ataskaitinį laikotarpį informacijos saugumo priemonių kiekis	
Nesėkmingai įdiegtų per ataskaitinį laikotarpį informacijos saugumo priemonių kiekis	
Nesėkmingai įdiegtų informacijos saugumo priemonių dalis bendrame planuotų priemonių kiekyje (%)	
Priimtinumas	
Informacijos saugumo incidentų valdymas	**Kartą per mėnesį, data**
Nustatytų informacijos saugumo įvykių kiekis	
Nustatytų informacijos saugumo incidentų kiekis	
Nustatytų pavojingų incidentų kiekis	
Incidentų kiekio padidėjimas ar sumažėjimas, palyginus su praeitu ataskaitiniu laikotarpiu (%)	
Priimtinumas	
Pavojingų incidentų dalis visų nustatytų per ataskaitinį laikotarpį incidentų kiekyje (%)	
Priimtinumas	
Neatitikčių valdymas	**Kartą per metus, data**
Nustatytų neatitikčių skaičius	
Išspręstų neatitikčių skaičius	
Nepašalintų neatitikčių skaičius	
Nepašalintų neatitikčių santykis (%)	
Priimtinumas	
Darbuotojų mokymų ir sąmoningumo informacijos saugumo srityje kėlimas	**Kartą per metus, data**
Numatytų pagal planą apmokyti darbuotojų kiekis	
Apmokytų darbuotojų kiekis	
Neapmokytų darbuotojų kiekis	

Neapmokytų darbuotojų dalis (%)	
Priimtinumas	
Saugumas, susijęs su išoriniais paslaugų tiekėjais	**Kartą per metus, data**
Sutarčių, pasirašytų su išoriniais paslaugų tiekėjais, skaičius	
Sutarčių, kuriose numatyti informacijos saugumo reikalavimai, skaičius	
Sutarčių, kuriose nenumatyti informacijos saugumo reikalavimai, skaičius	
Sutarčių, kuriose nenumatyti informacijos saugumo reikalavimai, dalis (%)	
Priimtinumas	
Veiklos tęstinumo valdymas	**Kartą per metus, data**
Informacinių sistemų ir registrų veiklos tęstinumo valdymo ir atkūrimo planų bandymų skaičius	
Sėkmingų informacinių sistemų ir registrų veiklos tęstinumo valdymo planų bandymų skaičius	
Nesėkmingų informacinių sistemų ir registrų veiklos tęstinumo valdymo planų bandymų skaičius	
Priimtinumas	
Numatyta veiklos tęstinumo atstatymo trukmė	
Nustatyta veiklos atstatymo trukmė	
Nustatytos veiklos atstatymo trukmės viršijimas (%)	
Priimtinumas	

Informacijos apsaugos priemonių
veiksmingumo matavimo proceso
2 priedas

(Informacijos saugumo dokumentų aktualumo ir priežiūros veiksmingumo matavimo klausimyno forma)

Klausimas	**Atsakymas**	**Komentaras**
Ar su informacijos saugumo valdymu susijusi dokumentacija peržiūrėta?		
Ar yra įrašai apie dokumentacijos peržiūrą?		
Ar yra neperžiūrėtų ISVS dokumentų?		
Ar ISVS dokumentacija atnaujinta?		
Ar atnaujinti įrašai, susiję su ISVS?		

Informacijos apsaugos priemonių
veiksmingumo matavimo proceso
3 priedas

(Mobiliųjų įrenginių naudojimo veiksmingumo matavimo klausimyno forma)

Klausimas	**Atsakymas**	**Komentaras**
Ar visi tikrinti mobilieji įrenginiai turi ekrano užsklandą?		
Ar visuose tikrintuose mobiliuosiuose įrenginiuose yra įdiegta antivirusinė programa?		
Kokia procentinė dalis tikrintų mobiliųjų įrenginių atitinka informacijos saugumo reikalavimus?		
Kokia procentinė dalis tikrintų mobiliųjų įrenginių neatitinka informacijos saugumo reikalavimų?		

Informacijos apsaugos priemonių
veiksmingumo matavimo proceso
4 priedas

(Prieigos valdymo veiksmingumo matavimo klausimyno forma)

Klausimas	**Atsakymas**	**Komentaras**
Ar tikrinant prieigos teises nustatyta, kad yra nebedirbančių Komisijoje darbuotojų, turinčių prieigos teises?		
Kokia procentinė dalis darbuotojų, nebedirbančių Komisijoje, turi prieigos teises?		
Koks nustatytų slaptažodžių skaičius?		
Kiek slaptažodžių atitinka nustatytus reikalavimus?		
Kokia procentinė dalis visų slaptažodžių atitinka nustatytus reikalavimus?		
Ar atitinkančių reikalavimus procentinė dalis yra nuo 60% iki 80%?		
Ar atitinkančių reikalavimus procentinė dalis yra mažesnė nei 60%?		
Koks priimtinumo kriterijus pagal nustatytą veiksmingumo matavimo procedūrą (priimtinas, nepriimtinas, pavojingas)?		
Ar reikia imtis papildomų veiksmų? (Jei taip, komentare nurodyti kokių)		

Informacijos apsaugos priemonių
veiksmingumo matavimo proceso
5 priedas

(Informacijos apsaugos valdymo priemonių įgyvendinimo veiksmingumo matavimo klausimyno forma)

Klausimas	Atsakymas	Komentaras
Koks patvirtintas rizikos valdymo plane reikalingų įgyvendinti informacijos saugumo valdymo priemonių skaičius?		
Koks pagal rizikos valdymo planą sėkmingai įgyvendintų saugumo valdymo priemonių skaičius?		
Kiek valdymo priemonių įgyvendinta vėliau nei buvo planuota?		
Kiek valdymo priemonių įgyvendinta žymiai (daugiau nei 20%) viršijant planuotus išteklius?		
Ar nesėkmingai įgyvendintų (jei tokių yra) saugumo valdymo priemonių procentinė dalis bendrame planuotų priemonių kiekyje viršija 20%?		
Koks priimtinumo kriterijus pagal nustatytą veiksmingumo matavimo procedūrą (priimtinas, nepriimtinas, pavojingas)?		
Ar reikia imtis papildomų veiksmų? (Jei taip, komentare nurodyti kokių)		

Informacijos apsaugos priemonių
veiksmingumo matavimo proceso
6 priedas

(Informacijos saugumo incidentų valdymo veiksmingumo matavimo klausimyno forma)

Klausimas	Atsakymas	Komentaras
Koks informacijos saugumo incidentų skaičius per praėjusį ataskaitinį laikotarpį?		
Koks informacijos saugumo incidentų skaičius per ataskaitinį laikotarpį?		
Koks informacijos saugumo incidentų skaičiaus procentinis pokytis, lyginant su praėjusiu ataskaitiniu laikotarpiu?		
Jei informacijos saugumo incidentų skaičius padidėjo, ar procentinis pokytis didesnis nei 50% ir mažesnis nei100%, lyginant su praėjusiu ataskaitiniu laikotarpiu?		
Jei informacijos saugumo incidentų skaičius padidėjo, ar procentinis pokytis viršija 100% lyginant su praėjusiu ataskaitiniu laikotarpiu?		
Koks priimtinumo kriterijus pagal nustatytą veiksmingumo matavimo procedūrą (priimtinas, nepriimtinas, pavojingas)?		
Ar reikia imtis papildomų veiksmų? (Jei taip, komentare nurodyti kokių)		
Koks kritinių informacijos saugumo incidentų skaičius per ataskaitinį laikotarpį?		
Kokia kritinių informacijos saugumo incidentų procentinė dalis bendrame užregistruotų informacijos saugumo incidentų skaičiuje?		
Ar kritinių informacijos saugumo incidentų procentinė dalis bendrame užregistruotų informacijos saugumo incidentų skaičiuje neviršija 20%?		
Ar kritinių informacijos saugumo incidentų procentinė dalis bendrame užregistruotų informacijos saugumo incidentų skaičiuje tarp 20% ir 50%?		
Ar kritinių informacijos saugumo incidentų procentinė dalis bendrame užregistruotų informacijos saugumo incidentų skaičiuje viršija 50%?		
Koks priimtinumo kriterijus pagal nustatytą veiksmingumo matavimo procedūrą (priimtinas, nepriimtinas, pavojingas)?		
Ar reikia imtis papildomų veiksmų? (Jei taip, komentare nurodyti kokių)		

Informacijos apsaugos priemonių
veiksmingumo matavimo proceso
7 priedas

(Informacijos saugumo valdymo sistemos neatitikčių šalinimo veiksmingumo matavimo klausimyno forma)

Klausimas	**Atsakymas**	**Komentaras**
Koks nustatytų neatitikčių per ataskaitinį laikotarpį skaičius?		
Koks sėkmingai pašalintų neatitikčių skaičius?		
Koks skaičius neatitikčių, kurios nepašalintos laiku?		
Koks skaičius neatitikčių, kurių pašalinimas žymiai (virš 20%) viršijo planuotus išteklius neatitikties šalinimui?		
Kokia nesėkmingai pašalintų neatitikčių procentinė dalis bendrame neatitikčių kiekyje?		
Ar nesėkmingai nepašalintų neatitikčių procentinė dalis bendrame neatitikčių skaičiuje neviršija 20%?		
Ar nesėkmingai nepašalintų neatitikčių procentinė dalis bendrame neatitikčių skaičiuje viršija 20%?		
Koks priimtinumo kriterijus pagal nustatytą veiksmingumo matavimo procedūrą (priimtinas, nepriimtinas, pavojingas)?		
Ar reikia imtis papildomų veiksmų? (Jei taip, komentare nurodyti kokių)		

Informacijos apsaugos priemonių
veiksmingumo matavimo proceso
8 priedas

(Darbuotojų mokymų ir sąmoningumo informacijos saugumo srityje valdymo veiksmingumo matavimo klausimyno forma)

Klausimas	Atsakymas	Komentaras
Kiek informacijos saugumo mokymo plane numatyta apmokyti darbuotojų?		
Apmokytų darbuotojų skaičius?		
Koks nedalyvavusių mokymuose darbuotojų skaičius?		
Ar apmokytų pagal planą darbuotojų dalis yra nuo 60% iki 80%?		
Ar apmokytų pagal planą darbuotojų dalis yra mažesnė nei 60%?		
Koks priimtinumo kriterijus pagal nustatytą veiksmingumo matavimo procedūrą (priimtinas, nepriimtinas, pavojingas)?		
Ar reikia imtis papildomų veiksmų? (Jei taip, komentare nurodyti kokių)		

Informacijos apsaugos priemonių
veiksmingumo matavimo proceso
9 priedas

(Saugumo, susijusio su išoriniais paslaugų tiekėjais, valdymo veiksmingumo matavimo klausimyno forma)

Klausimas	Atsakymas	Komentaras
Koks pasirašytų su išoriniais paslaugų tiekėjais sutarčių skaičius?		
Kiek yra sutarčių su išoriniais paslaugų tiekėjais, kuriose numatyti informacijos saugumo reikalavimai?		
Kokia procentinė dalis sutarčių, kuriose numatyti informacijos saugumo reikalavimai visame pasirašytų su išoriniais paslaugų tiekėjais skaičiuje?		
Ar sutarčių su išoriniais paslaugų tiekėjais, kuriose nėra numatytų informacijos saugumo reikalavimų procentinė dalis visame pasirašytų sutarčių skaičiuje viršija 20%?		
Koks priimtinumo kriterijus pagal nustatytą veiksmingumo matavimo procedūrą (priimtinas, nepriimtinas, pavojingas)?		
Ar reikia imtis papildomų veiksmų? (Jei taip, komentare nurodyti kokių)		

Informacijos apsaugos priemonių
veiksmingumo matavimo proceso
10 priedas

(Veiklos tęstinumo valdymo veiksmingumo matavimo klausimyno forma)

Klausimas	**Atsakymas**	**Komentaras**
Ar atliekami veiklos tęstinumo valdymo planų bandymai?		
Kiek buvo sėkmingų veiklos tęstinumo valdymo planų bandymų?		
Kiek buvo nesėkmingų veiklos tęstinumo valdymo planų bandymų?		
Ar visi veiklos tęstinumo valdymo planų bandymai buvo nesėkmingi?		
Koks priimtinumo kriterijus pagal nustatytą veiksmingumo matavimo procedūrą (priimtinas, nepriimtinas, pavojingas)?		
Ar reikia imtis papildomų veiksmų? (Jei taip, komentare nurodyti kokių)		
Kokia nustatyta veiklos atkūrimo trukmė pagal planą?		
Ar išmatuota veiklos atkūrimo trukmė neviršija nustatytos pagal planą?		
Ar išmatuota veiklos atkūrimo trukmė viršija nustatytą pagal veiklos atstatymo planą iki 50%?		
Ar išmatuota veiklos atkūrimo trukmė viršija nustatytą pagal veiklos atstatymo planą virš 50%?		
Koks priimtinumo kriterijus pagal nustatytą veiksmingumo matavimo procedūrą (priimtinas, nepriimtinas, pavojingas)?		
Ar reikia imtis papildomų veiksmų? (Jei taip, komentare nurodyti kokių)		