LIETUVOS AUTOMOBILIŲ KELIŲ DIREKCIJOS PRIE SUSISIEKIMO MINISTERIJOS DIREKTORIUS

ĮSAKYMAS
DĖL VALSTYBINĖS REIKŠMĖS KELIŲ EISMO INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLIŲ, VALSTYBINĖS REIKŠMĖS KELIŲ EISMO INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLIŲ IR VALSTYBINĖS REIKŠMĖS KELIŲ EISMO INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANO PATVIRTINIMO

2016 m. birželio 16 d. Nr. V-332
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 8 punktu ir Saugos dokumentų turinio gairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, ir atsižvelgdamas į Valstybinės reikšmės kelių eismo informacinės sistemos nuostatus ir Valstybinės reikšmės kelių eismo informacinės sistemos duomenų saugos nuostatus, patvirtintus Lietuvos automobilių kelių direkcijos prie Susisiekimo ministerijos direktoriaus 2016 m. vasario 17 d. įsakymu Nr. V-126 „Dėl Valstybinės reikšmės kelių eismo informacinės sistemos nuostatų ir Valstybinės reikšmės kelių eismo informacinės sistemos duomenų saugos nuostatų patvirtinimo“,

t v i r t i n u pridedamus:

1. Valstybinės reikšmės kelių eismo informacinės sistemos saugaus elektroninės informacijos tvarkymo taisykles.
2. Valstybinės reikšmės kelių eismo informacinės sistemos naudotojų administravimo taisykles.
3. Valstybinės reikšmės kelių eismo informacinės sistemos veiklos tęstinumo valdymo planą.

Direktorius Egidijus Skrodenis

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2016 m. birželio 9 d. raštu Nr. 1D-3690

PATVIRTINTA
Lietuvos automobilių kelių direkcijos prie
Susisiekimo ministerijos direktoriaus
2016 m. birželio 16 d.
įsakymu Nr. V-332

VALSTYBINĖS REIKŠMĖS KELIŲ EISMO INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės reikšmės kelių eismo informacinės sistemos naudotojų administravimo taisyklės (toliau – Taisyklės) nustato Valstybinės reikšmės kelių eismo informacinės sistemos (toliau – EIS) naudotojų ir administratorių įgaliojimus, teises ir pareigas ir saugaus duomenų teikimo EIS naudotojams kontrolės tvarką.

2. Šios Taisyklės parengtos vadovaujantis Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“, Valstybinės reikšmės kelių eismo informacinės sistemos nuostatais ir Valstybinės reikšmės kelių eismo informacinės sistemos duomenų saugos nuostatais, patvirtintais Lietuvos automobilių kelių direkcijos prie Susisiekimo ministerijos direktoriaus 2016 m. vasario 17 d. įsakymu Nr. V-126 „Dėl Valstybinės reikšmės kelių eismo informacinės sistemos nuostatų ir Valstybinės reikšmės kelių eismo informacinės sistemos duomenų saugos nuostatų patvirtinimo“.

3. Taisyklėse vartojamos sąvokos atitinka Taisyklių 2 punkte nurodytuose teisės aktuose apibrėžtas sąvokas.

4. Taisyklės taikomos visiems EIS naudotojams, administratoriui ir saugos įgaliotiniui.

5. EIS naudotojams prieiga prie EIS duomenų suteikiama vadovaujantis šiais principais:

5.1. EIS naudotojams prieiga turi būti suteikiama tik prie tų EIS duomenų ir tik tokios apimties, kuri reikalinga EIS naudotojo pareigybės aprašyme nurodytoms funkcijoms atlikti;

5.2. EIS duomenis gali keisti (sukurti, papildyti ar panaikinti) tik tokią teisę turintys EIS naudotojai;

5.3. prieiga prie EIS duomenų ir teisė juos keisti suteikiama tik atlikus EIS naudotojo identifikaciją ir patvirtinus jo tapatybę; asmens kodas negali būti naudojamas kaip EIS naudotojo identifikatorius;

5.4. kiekvienas EIS naudotojas turi būti informacinėje sistemoje unikaliai identifikuojamas (asmens kodas negali būti naudojamas kaip informacinės sistemos naudotojo identifikatorius);

5.5. EIS naudotojams negali būti suteikiamos administratoriaus teisės.

II SKYRIUS
EIS ADMINISTRATORIAUS IR NAUDOTOJŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

6. EIS naudotojai turi teisę:

6.1. naudotis tik tomis EIS funkcijomis ir EIS duomenimis, prie kurių prieigą jiems suteikė administratorius;

6.2. gauti informaciją apie jų naudojamų EIS duomenų apsaugos lygį ir taikomas apsaugos priemones, teikti pasiūlymus dėl papildomų apsaugos priemonių;

6.3. kreiptis į administratorių ar EIS saugos įgaliotinį dėl neveikiančios ar netinkamai veikiančios EIS.

7. EIS naudotojai privalo:

7.1. naudoti EIS duomenis tik tarnybinėms funkcijoms atlikti;

7.2. pranešti administratoriui apie EIS saugos politikos įgyvendinamųjų teisės aktų pažeidimus, veiksmus, turinčius nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones;

7.3. užtikrinti jų naudojamų EIS duomenų konfidencialumą ir vientisumą, savo veiksmais netrikdyti EIS duomenų prieinamumo;

7.4. susipažinti ir laikytis Valstybinės reikšmės kelių eismo informacinės sistemos nuostatų, patvirtintų Lietuvos automobilių kelių direkcijos prie Susisiekimo ministerijos direktoriaus 2016 m. vasario 17 d. įsakymu Nr. V-126 „Dėl Valstybinės reikšmės kelių eismo informacinės sistemos nuostatų ir Valstybinės reikšmės kelių eismo informacinės sistemos duomenų saugos nuostatų patvirtinimo“ (toliau – EIS saugos nuostatai), Valstybinės reikšmės kelių eismo informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių, EIS informacinės sistemos veiklos tęstinumo valdymo plano, šių Taisyklių ir kitų EIS informacijos saugos įgyvendinamųjų teisės aktų reikalavimų;

7.5. raštu pranešti administratoriui apie slaptažodžio užblokavimą ar užmiršimą;

7.6. baigus darbą ar pasitraukiant iš darbo vietos EIS imtis priemonių, kad su EIS tvarkomais asmens duomenimis negalėtų susipažinti pašaliniai asmenys: atsijungti nuo EIS, įjungti slaptažodžiu apsaugotą ekrano užsklandą.

8. EIS naudotojui draudžiama:

8.1. leisti prisijungti prie EIS ne EIS naudotojui ar kitais nei šiose Taisyklėse nustatytais būdais;

8.2. be priežiūros palikti kompiuterį, neatsijungus nuo EIS;

8.3. platinti EIS esančią informaciją, daryti jos kopijas ar kitu būdu ją dauginti.

9. Administratorius turi teisę:

9.1. matyti visų EIS naudotojų identifikavimo ir suteiktų teisių duomenis;

9.2. matyti EIS naudotojų su EIS duomenimis atliktus redagavimo veiksmus;

9.3. atlikti užklausas EIS pagal pasirinktus paieškos kriterijus;

9.4. pateikti paklausimus dėl EIS naudotojų duomenų patikslinimo;

9.5. fiziškai prieiti prie techninės ir sisteminės programinės įrangos;

9.6. vykdyti EIS techninės priežiūros funkcijas.

10. Administratorius privalo:

10.1. registruoti naujus EIS naudotojus ;

10.2. tvarkyti esamų EIS naudotojų duomenis (pagal EIS valdytojo ir EIS tvarkytojo pateiktus duomenis);

10.3. tvarkyti EIS vidinius klasifikatorius, esančius EIS klasifikatorių funkciniame modulyje;

10.4. konsultuoti EIS naudotojus dėl EIS veikimo ir kitais su EIS susijusiais klausimais;

10.5. pagal kompetenciją užtikrinti nepertraukiamą EIS techninės ir sisteminės programinės įrangos veikimą;

10.6. dalyvauti atliekant EIS rizikos veiksnių įvertinimą ir rengiant EIS rizikos veiksnių įvertinimo ataskaitą ir rizikos veiksnių įvertinimo ir rizikos veiksnių valdymo priemonių planą;

10.7. atlikti EIS taikomų saugumo reikalavimų atitikties vertinimą.

11. Administratoriui draudžiama suteikti EIS duomenų redagavimo teises ne EIS naudotojams.

12. Administratoriaus funkcijos reglamentuotos EIS saugos nuostatuose ir kituose EIS saugos politikos įgyvendinamuosiuose teisės aktuose.

13. Saugos įgaliotinio funkcijos reglamentuotos EIS saugos nuostatuose ir kituose EIS saugos politikos įgyvendinamuosiuose teisės aktuose.

14. EIS naudotojas, norėdamas gauti prieigos prie EIS duomenų teisę, asmeniškai arba per kelius prižiūrinčias valstybės įmones administratoriui teikia prašymą, kuriame nurodo savo pareigas, vardą, pavardę. Administratorius per 2 darbo dienas nuo prašymo gavimo dienos pritaria prašymui ir suteikia EIS naudotojui prieigos prie EIS duomenų teisę arba nepritaria prašymui. Administratoriui teikiamas naudotojo prašymas turi būti vizuotas naudotojo tiesioginio vadovo.

III SKYRIUS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO EIS NAUDOTOJAMS KONTROLĖS TVARKA

15. Administratorius yra atsakingas už EIS naudotojų registravimą, išregistravimą, prieigos prie EIS teisių suteikimą ir panaikinimą.

16. Administratorius EIS naudotojams suteikia unikalius prisijungimo prie EIS vardą ir laikiną slaptažodį, kurį išsiunčia EIS naudotojui elektroniniu paštu.

17. EIS naudotojai prisijungti prie EIS gali tik su administratoriaus suteiktais unikaliais vardais ir slaptažodžiais.

18. EIS naudotojų prisijungimo prie EIS vardai ir slaptažodžiai saugomi EIS naudotojų prisijungimo vardų ir slaptažodžių elektroninėje saugykloje (toliau – saugykla).

19. Prieigą prie saugyklos turi tik administratorius. Duomenys saugykloje yra šifruojami.

20. Prisijungti nuotoliniu būdu prie EIS galima naudojant protokolą, skirtą duomenims šifruoti.

21. Slaptažodį EIS naudotojai turi teisę savarankiškai pasikeisti prisijungę prie EIS.

22. EIS naudotojo slaptažodžiui yra keliami šie reikalavimai:

22.1. slaptažodis turi būti iš ne trumpesnės kaip 8 simbolių kombinacijos, sudarytos iš didžiųjų ir mažųjų raidžių, skaičių ir specialiųjų simbolių;

22.2. slaptažodžiams neturi būti naudojama asmeninio pobūdžio informacija;

22.3. slaptažodis turi būti keičiamas ne rečiau kaip kas 3 mėnesius;

22.4. keičiant slaptažodį neleidžiama pasirinkti slaptažodžio iš paskutiniųjų 6 slaptažodžių;

22.5. EIS naudotojas, pirmą kartą gavęs administratoriaus suteiktą vardą ir slaptažodį, turi prisijungti prie EIS ir nedelsdamas slaptažodį pakeisti;

22.6. EIS naudotojas privalo saugoti slaptažodį ir jo neatskleisti tretiesiems asmenims;

22.7. EIS naudotojas, įtaręs, kad tretieji asmenys sužinojo slaptažodį, privalo nedelsdamas jį pakeisti;

22.8. EIS naudotojas neturi teisės užrašyto slaptažodžio palikti matomoje vietoje;

22.9. didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius – 3 kartai. EIS naudotojui 3 kartus neteisingai įvedus slaptažodį EIS užsirakina ir EIS naudotojui 10 minučių neleidžiama identifikuotis;

22.10. EIS moduliai, atliekantys nutolusio prisijungimo prie EIS autentifikavimą, turi neleisti automatiškai išsaugoti slaptažodžių;

22.11. slaptažodžiai negali būti saugomi ar perduodami atviru tekstu ar užšifruojami nepatikimais algoritmais; saugos įgaliotinio sprendimu tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jei EIS naudotojas neturi

galimybių iššifruoti gauto užšifruoto slaptažodžio arba jei nėra galimybių EIS naudotojui perduoti slaptažodžius šifruotu kanalu ar saugiu elektroninių ryšių tinklu.

23. Administratoriaus slaptažodžiui yra keliami šie reikalavimai:

23.1. administratoriaus slaptažodis turi būti iš ne trumpesnės kaip 12 simbolių kombinacijos, sudarytos iš didžiųjų, mažųjų raidžių, skaitmenų ir specialiųjų simbolių;

23.2. administratoriaus slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius;

23.3. keičiant slaptažodį neleidžiama pasirinkti slaptažodžio iš buvusių 3 paskutinių slaptažodžių.

24. Administratorius, iš valdytojo gavęs prašymą apriboti EIS naudotojo prieigos teises, nedelsdamas apriboja nurodyto EIS naudotojo prieigą prie EIS.

25. EIS naudotojui teisė dirbti su konkrečia elektronine informacija yra sustabdoma, kai vyksta EIS naudotojo veiklos tyrimas.

26. Kai EIS naudotojas perkeliamas į kitas pareigas, jam suteiktos EIS naudotojo teisės pakeičiamos atsižvelgiant į jo pareigybės aprašyme nurodytas funkcijas.

27. EIS naudotojui teisė naudotis EIS panaikinama arba sustabdoma:

27.1. pasibaigus tarnybos ar darbo santykiams;

27.2. netekus teisės naudotis EIS duomenimis;

27.3. nustačius neteisėtą EIS naudotojo EIS duomenų naudojimą;

27.4. kai nesinaudoja EIS ilgiau kaip 3 mėnesius.

_____

PATVIRTINTA
Lietuvos automobilių kelių direkcijos prie
Susisiekimo ministerijos direktoriaus
2016 m. birželio 16 d.
įsakymu Nr. V-332

VALSTYBINĖS REIKŠMĖS KELIŲ EISMO INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I. SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės reikšmės kelių eismo informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) reglamentuoja tvarką, užtikrinančią saugų Valstybinės reikšmės kelių eismo informacinės sistemos (toliau – EIS) techninės, programinės įrangos funkcionavimą, saugų EIS duomenų tvarkymą ir jų teikimą duomenų gavėjams pagal teisės aktų nustatytus reikalavimus.

2. Šios Taisyklės parengtos vadovaujantis Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“, Valstybinės reikšmės kelių eismo informacinės sistemos nuostatais ir Valstybinės reikšmės kelių eismo informacinės sistemos duomenų saugos nuostatais, patvirtintais Lietuvos automobilių kelių direkcijos prie Susisiekimo ministerijos direktoriaus 2016 m. vasario 17 d. įsakymu Nr. V-126 „Dėl Valstybinės reikšmės kelių eismo informacinės sistemos nuostatų ir Valstybinės reikšmės kelių eismo informacinės sistemos duomenų saugos nuostatų patvirtinimo“.

3. Taisyklėse vartojamos sąvokos atitinka Taisyklių 2 punkte nurodytuose teisės aktuose apibrėžtas sąvokas.

4. EIS saugoma informacija yra skirstoma į šias grupes:

4.1. administratoriaus tvarkoma informacija;

4.2. EIS naudotojų tvarkoma informacija;

4.3. iš daviklių gaunami duomenys.

5. Elektroninės informacijos, priskirtos Taisyklių 4 punkte nurodytoms grupėms, sąrašas:

5.1. EIS administratoriaus tvarkoma informacija:

5.1.1. EIS konfigūracijos parametrai;

5.1.2. EIS klasifikatoriai;

5.1.3. EIS naudotojų teisės;

5.1.4. EIS techninės ir programinės įrangos parametrai;

5.1.5. elektroninių paslaugų inicijavimo ir teikimo duomenys;

5.1.6. elektroninių paslaugų teikimo stebėsenos duomenys;

5.1.7. rezervinės kopijos;

5.2. EIS naudotojų tvarkoma informacija:

5.2.1. metaduomenys;

5.2.2. erdvinių duomenų paslaugų tvarkymo duomenys;

5.2.3. EIS svetainės www.eismoinfo.lt eismo sąlygų ir naujienų pranešimai ir kiti turinio duomenys.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

6. Saugiam EIS elektroninės informacijos tvarkymui užtikrinti naudojamos kompiuterinės įrangos, programinės įrangos, duomenų perdavimo tinklai, fizinės, techninės ir organizacinės duomenų saugumo priemonės.

7. Kompiuterinės įrangos saugos priemonės:

7.1. prieigos prie EIS tarnybinių stočių (serverių) kontrolė, užtikrinama suteikiant prieigos prie EIS tarnybinių stočių teises tik EIS administratoriui ir už EIS priežiūrą atsakingos įmonės darbuotojui;

7.2. svarbiausia kompiuterinė įranga, duomenų perdavimo tinklo mazgai ir ryšio linijos privalo būti dubliuoti ir jų techninė būklė nuolat stebima;

7.3. kompiuterinės įrangos sujungimas klasteriniu režimu (angl. *computer cluster*), t. y. kompiuterinės įrangos dubliavimas ir šios kompiuterinės įrangos techninės būklės nuolatinė stebėsena;

7.4. EIS naudotojų naudojamos techninės kompiuterinės įrangos priežiūra ir tvarkymas, kurią atlieka EIS valdytojas ir tvarkytojas;

7.5. kompiuterinės įrangos gedimų registravimas kompiuterinės įrangos gedimų žurnale.

8. EIS sisteminės ir taikomosios programinės įrangos (toliau – EIS programinė įranga) saugos priemonės:

8.1. naudojama legali programinė įranga;

8.2. programinės įrangos diegimą atlieka tik asmenys, turintys teisę ir gebėjimų diegti programinę įrangą;

8.3. EIS naudojamos autorizuotos programinės įrangos sąrašo rengimas ir reguliarus atnaujinimas, už kurį atsakingas EIS valdytojas;

8.4. neautorizuotos programinės įrangos įdiegimo į EIS naudotojų kompiuterius ribojimas ir nuolatinis EIS programinės įrangos stebėsenos vykdymas, už kurį atsakingas EIS valdytojas;

8.5. EIS tarnybinėse stotyse ir kompiuterinėse EIS naudotojų darbo vietose naudojamos centralizuotai valdomos kenksmingosios programinės įrangos aptikimo priemonės, kurios yra automatiniu būdu atnaujinamos ne rečiau kaip kartą per 10 dienų;

8.6. prisijungimo duomenis, suteikiančius teisę dirbti su EIS tarnybinėmis stotimis ir jų administravimo programine įranga, gali žinoti tik administratorius ir EIS priežiūrą atliekančios įmonės darbuotojas;

8.7. prieigos teisė dirbti su EIS programine įranga suteikiama EIS naudotojams Valstybinės reikšmės kelių eismo informacinės sistemos naudotojų administravimo taisyklių, (toliau – EIS naudotojų administravimo taisyklės), nustatyta tvarka;

8.8. EIS naudotojams jų naudojamų kompiuterių operacinėse sistemose suteikiamos tik tiesioginėms pareigoms vykdyti būtinos teisės;

8.9. EIS naudotojų tapatybei, EIS naudotojų veiksmams, atliekamiems EIS, nustatyti taikomos programinės priemonės;

8.10. administratoriaus perspėjimo programinės priemonės, perspėjančios sumažėjus iki nustatytos pavojingos ribos EIS tarnybinių stočių laisvos operatyvios atminties, vietos standžiajame diske, taip pat kai ilgą laiką stipriai apkrautas centrinis procesorius arba kompiuterių tinklo sąsajos;

8.11. laikmenos su EIS programinės įrangos atsarginėmis kopijomis privalo būti laikomos nedegioje spintoje, kitose patalpose arba kitame pastate, nei yra EIS tarnybinės stotys;

8.12. EIS programinė įranga prižiūrima tik laikantis gamintojo rekomendacijų;

8.13. EIS naudotojų darbo vietose gali būti naudojamos tik tarnybinėms reikmėms skirtos išorinės duomenų laikmenos (pavyzdžiui, USB, CD, DVD ir kt.); šios laikmenos negali būti naudojamos veiklai, nesusijusiai su teisėtu informacinės sistemos tvarkymu.

9. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

9.1. EIS naudotojas internetu jungiasi prie užkarda (angl. *firewall*) apsaugotų tarnybinių stočių, kuriose yra EIS, naudodamas unikalius identifikacinius prisijungimo duomenis;

9.2. saugaus elektroninės informacijos teikimo ir (ar) gavimo iš kitų valstybės institucijų užtikrinimas, naudojant Saugų valstybės duomenų perdavimo tinklą (toliau – SVDPT);

9.3. EIS naudotojų kompiuterių tinklai privalo tenkinti SVDPT saugos organizavimo, valdymo ir SVDPT naudotojų prijungimo reikalavimus, nustatytus Saugaus valstybinio duomenų perdavimo tinklo elektroninės informacijos saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2007 m. birželio 5 d. įsakymu Nr. 1V-210 „Dėl Saugaus valstybinio duomenų perdavimo tinklo elektroninės informacijos saugos reikalavimų patvirtinimo“;

9.4. viešaisiais tinklais siunčiami EIS duomenys yra šifruojami;

9.5. EIS duomenų perdavimo tinklas privalo būti atskirtas nuo viešųjų ryšių tinklų užkarda; užkardos įvykių žurnalai (angl. *Logs*) privalo būti reguliariai analizuojami, o užkardos saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos;

9.6. prisijungti nuotoliniu būdu prie EIS galima naudojant protokolą, skirtą duomenims šifruoti.

10. Patalpų, kuriose yra EIS tarnybinės stotys (toliau – patalpos), ir aplinkos saugumo užtikrinimo priemonės:

10.1. privalo būti užtikrinamas išorės poveikio šaltinių – transporto priemonių keliamos vibracijos, eismo įvykių, radijo stočių, specialiųjų gamyklų, kitų išorės šaltinių minimalus poveikis patalpoms ir jose esančiai techninei ir programinei įrangai;

10.2. patalpose įrengta langų ir durų fizinė apsauga: prie langų pritvirtintos žaliuzės ir metalinės grotos, įrengtos rakinamos šarvuotos ir ugniai atsparios durys, veikia durų ir langų signalizacija;

10.3. patalpos atitinka gaisrinės saugos reikalavimus, jose yra pirminių gaisro gesinimo priemonių, kurių patikra atliekama ne rečiau kaip kartą per metus;

10.4. patalpose įrengti įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų;

10.5. patalpos atskirtos nuo bendrojo naudojimo patalpų;

10.6. patekti į patalpas gali tik EIS administratorius, o asmenys, nesusiję su EIS tarnybinių stočių administravimu, patekti į šias patalpas gali tik lydimi administratoriaus ir užsiregistravę patekimo į patalpas, kuriose yra EIS tarnybinės stotys, žurnale;

10.7. EIS tarnybinių stočių techninė įranga įnešama į patalpas ar išnešama iš patalpų leidus administratoriui;

10.8. EIS tarnybinių stočių techninė įranga apsaugoma nuo elektros srovės svyravimų; naudojami specialūs maitinimo šaltiniai, nenutrūkstamo maitinimo šaltinis su automatine apsauga nuo įtampos svyravimų;

10.9. rezervinio nenutrūkstamo maitinimo šaltinis užtikrina EIS tarnybinių stočių įrangos veikimą ne trumpiau nei 30 minučių pagrindinio nenutrūkstamo maitinimo šaltinio neveikimo atveju;

10.10. ryšių kabeliai apsaugoti nuo nesankcionuoto prisijungimo prie jų ir jų pažeidimo;

10.11. įgyvendintos gamintojo nustatytos EIS tarnybinių stočių techninės įrangos darbo sąlygos;

10.12. patalpose nuolat turi veikti oro temperatūros reguliavimo įranga (oro kondicionavimo sistema) ir palaikoma +22 (±5) ºC temperatūra ir 50 (±10) proc. santykinis oro drėgnumas.

11. EIS darbo apskaitos ir kitos elektroninės informacijos saugos priemonės:

11.1. programiniu būdu registruojami EIS naudotojų veiksmai, atliekami su EIS duomenimis;

11.2. EIS naudotojams suteikiamos minimalios prieigos prie EIS teisės tik tiesioginėms funkcijoms vykdyti;

11.3. EIS tarnybinių stočių įvykių žurnaluose privalo būti registruojami ir ne mažiau kaip vienerius metus saugomi duomenys apie EIS tarnybinių stočių, informacinės sistemos taikomosios programinės įrangos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis informacinės sistemos tarnybinėse stotyse, EIS taikomojoje programinėje įrangoje, visus EIS naudotojų vykdomus veiksmus, kitus elektroninės informacijos saugai svarbius įvykius, nurodant EIS naudotojo identifikatorių ir elektroninės informacijos saugai svarbaus įvykio ar vykdyto veiksmo laiką; šie duomenys privalo būti saugomi ne toje pačioje informacinėje sistemoje, kurioje jie įrašomi, taip pat jie privalo būti analizuojami ne rečiau kaip kartą per savaitę;

11.4. EIS naudotojų kompiuteriuose privalo būti įdiegtos ekrano užsklandos (angl. *Screensaver*), kurios privalo būti apsaugotos slaptažodžiu (režimo aktyvavimo laikas – ne daugiau kaip 10 minučių);

11.5. EIS atitikties vertinimas privalo būti atliekamas ne rečiau kaip kartą per metus.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

12. EIS duomenis keisti, atnaujinti, įrašyti ir naikinti gali tik EIS naudotojai, turintys teisę tai atlikti.

13. EIS privalo turėti įvestos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemones.

14. EIS tinkle privalo būti įdiegtos ir veikti automatinės įsilaužimo aptikimo sistemos.

15. EIS duomenys įrašomi, atnaujinami, keičiami ir naikinami vadovaujantis EIS nuostatais, Lietuvos automobilių kelių direkcijos prie Susisiekimo ministerijos direktoriaus 2016 m. vasario 17 d. įsakymu Nr. V-126 „Dėl Valstybinės reikšmės kelių eismo informacinės sistemos nuostatų ir Valstybinės reikšmės kelių eismo informacinės sistemos duomenų saugos nuostatų patvirtinimo“.

16. EIS naudotojų veiksmų registravimo tvarka:

16.1. EIS naudotojų tapatybė ir veiksmai su EIS duomenimis įrašomi automatiniu būdu EIS duomenų bazės veiksmų žurnale, apsaugotame nuo neteisėto jame esančių duomenų panaudojimo, pakeitimo, iškraipymo ar sunaikinimo;

16.2. EIS duomenų bazės veiksmų žurnalo duomenys prieinami tik administratoriui.

17. Prarasti, iškraipyti ar sunaikinti EIS duomenys atkuriami iš atsarginių EIS duomenų kopijų. Atsarginės EIS duomenų kopijos daromos, saugomos ir EIS duomenys atkuriami iš atsarginių duomenų kopijų tokia tvarka:

17.1. už atsarginių EIS duomenų kopijų darymą, duomenų atkūrimą ir atsarginių EIS duomenų kopijų apsaugą yra atsakingas administratorius;

17.2. EIS duomenys privalo būti kopijuojami ir saugomi tokios apimties, kad EIS duomenų praradimo atveju visišką EIS funkcionalumą ir veiklą būtų galima atkurti per 12 valandų;

17.3. EIS duomenys atsarginėse kopijose yra užšifruoti;

17.4. EIS duomenų atsarginių kopijų darymas fiksuojamas atsarginių kopijų darymo žurnale;

17.5. EIS duomenų saugykloje realiu laiku yra dubliuojami visi EIS duomenys;

17.6. visos EIS duomenų kopijos į rezervinio kopijavimo biblioteką perkeliamos vieną kartą per 24 valandas;

17.7. EIS duomenų kopijos saugomos užrakintoje nedegioje spintoje, esančioje kitose patalpose, nei yra EIS tarnybinių stočių įrenginys, kurio elektroninė informacija buvo nukopijuota; patekti į patalpas gali tik administratorius, o asmenys, nesusiję su atsarginių EIS duomenų kopijų saugojimu, patekti į šias patalpas gali tik lydimi administratoriaus ir užsiregistravę patekimo į patalpas, kuriose yra EIS duomenų kopijos, žurnale;

17.8. administratorius kartą per savaitę atsargines EIS duomenų kopijas perkelia į saugojimo vietą;

17.9. visiški ir daliniai EIS duomenų atkūrimo bandymai atliekami vieną kartą per metus;

17.10. visiški ir daliniai EIS duomenų atkūrimo bandymai atliekami ne darbo valandomis ir prieš tai informavus visus EIS naudotojus;

17.11. už visiškus ir dalinius EIS duomenų atkūrimo bandymus yra atsakingi administratorius ir saugos įgaliotinis; administratorius su saugos įgaliotiniu parengia ir suderina visiško ir dalinio EIS duomenų atkūrimo bandymų metodus ir užtikrina atsarginių EIS duomenų kopijų saugojimą ir atsarginių EIS duomenų kopijų darymo kontrolę.

18. EIS duomenų perkėlimo ir teikimo kitoms informacinėms sistemoms, duomenų gavimo iš jų tvarka:

18.1. už EIS naudotojų administravimą ir iš valstybės registrų ir kitų susijusių informacinių sistemų teikiamų duomenų atnaujinimą EIS yra atsakingas administratorius;

18.2. duomenų mainai tarp EIS ir kitų informacinių sistemų vykdomi su šių informacinių sistemų valdytojais sudarytose duomenų teikimo sutartyse numatytais būdais, terminais ir numatytos apimties;

18.3. reorganizuojant arba likviduojant EIS, jos elektroninė informacija privalo būti saugiai perduota kitai informacinei sistemai, valstybės archyvams arba sunaikinama Lietuvos Respublikos dokumentų ir archyvų įstatymo nustatyta tvarka.

19. Duomenų neteisėto kopijavimo, keitimo, naikinimo ar perdavimo (toliau – neteisėti veiksmai) nustatymo tvarka:

19.1. administratorius, užtikrindamas EIS duomenų vientisumą, privalo naudoti visas įmanomas fizines, programines ir organizacines priemones, skirtas EIS ir joje tvarkomiems duomenims apsaugoti nuo neteisėtų veiksmų;

19.2. EIS naudotojas, įtaręs, kad su EIS duomenimis buvo atlikti ar yra atliekami neteisėti veiksmai, privalo pranešti apie tai administratoriui; administratorius, atsiradus įtarimų dėl neteisėtų veiksmų su EIS duomenimis, pasinaudojęs EIS duomenų bazės veiksmų žurnalo įrašais, nustato neteisėto poveikio šaltinį, laiką ir veiksmus, atliktus su EIS programine įranga ir (ar) duomenimis;

19.3. administratorius, įtaręs, kad su EIS duomenimis atliekami neteisėti veiksmai, privalo apie tai pranešti saugos įgaliotiniui;

19.4. saugos įgaliotinis, gavęs administratoriaus pranešimą apie įvykdytus ar vykdomus neteisėtus veiksmus su EIS arba su EIS tvarkomais duomenimis, inicijuoja elektroninės informacijos saugos incidento valdymo procedūras, nustatytas EIS veiklos tęstinumo valdymo plane.

20. EIS programinės ir techninės įrangos keitimo ir atnaujinimo tvarka:

20.1. EIS tarnybinėse stotyse programinę įrangą, reikalingą EIS darbui, diegia ir tvarko EIS administratorius;

20.2. organizuojami EIS naudotojų darbo su nauja programine ir technine įranga mokymai;

20.3. naudojama tik sertifikuota programinė ir techninė įranga;

20.4. sugedusią techninę įrangą išvežant remontuoti, išimamos duomenų laikmenos (kietieji diskai ir kt.) arba daromos jų kopijos ir laikmenose saugomi duomenys ištrinami;

20.5. techninės, programinės ir sisteminės įrangos naujinimui galioja pokyčių valdymo tvarka;

20.6. EIS programinės ir techninės įrangos keitimo ir atnaujinimo tvarką su trečiąja šalimi, jei šiai šaliai Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka perduotos informacinės sistemos ir (ar) jos infrastruktūros priežiūros funkcijos (toliau – paslaugų teikėjas), priklausomai nuo konkretaus atvejo, derina EIS administratorius arba ji aprašoma paslaugų, susijusių su EIS programinės ir techninės įrangos keitimu ir atnaujinimu, teikimo sutartyse.

21. EIS pokyčių valdymo tvarka:

21.1. EIS valdytojas užtikrina EIS pokyčių (toliau − pokyčiai) valdymo planavimą, apimantį pokyčių identifikavimą, suskirstymą į kategorijas pagal pokyčio tipą (administracinis, organizacinis ar techninis), įtakos vertinimą (svarbumas ir skubumas), pokyčių prioritetų nustatymo (eiliškumas) procesus;

21.2. pokyčiai identifikuojami nustačius EIS naudotojų, EIS administratorių poreikius, apibendrinus kylančias priežiūros problemas ir kitais gerosios praktikos įvardijamais atvejais;

21.3. visi potencialūs pokyčiai registruojami pokyčių registre, įvertinus ir valdytojui patvirtinus įtakos vertinimą ir prioritetą;

21.4. visi pokyčiai (projektavimas, kūrimas, testavimas, diegimas) atliekami tik EIS valdytojo, EIS saugos įgaliotinio ar EIS administratoriaus iniciatyva;

21.5. pokyčių projektavimą ir kūrimą atlieka Lietuvos automobilių kelių direkcijos prie Susisiekimo ministerijos Intelektinių transporto sistemų skyriaus darbuotojas, pagal pareigybės aprašymą atsakingas už taikomosios programinės įrangos priežiūrą ir projektavimą tam skirtoje kūrimo aplinkoje, reikalui esant pasitelkdamas trečiąsias šalis;

21.6. prieš atliekant pokyčius, kurių metu gali iškilti grėsmė elektroninės informacijos konfidencialumui, vientisumui ar pasiekiamumui, visi pokyčiai privalo būti išbandomi testavimo aplinkoje, kuri yra identiška gamybinei aplinkai;

21.7. įgyvendinant pokyčius, kurių metu galimi EIS veikimo sutrikimai, EIS administratorius privalo ne vėliau kaip prieš dvi darbo dienas iki planuojamų pokyčių pradžios (elektroniniu paštu, faksu ar kitomis priemonėmis) informuoti EIS saugos įgaliotinį ir naudotojus apie tokių darbų pradžią ir galimus sutrikimus;

21.8. atlikęs pokyčių testavimą, jei ir testavimo darbų dėl programinių ir (ar) techninių priežasčių nebuvo galima atlikti, EIS administratorius gali pradėti eksploatuoti pakeitimus;

21.9. jeigu testavimas sėkmingas, pokyčiai perkeliami į gamybinę aplinką;

21.10. visi pokyčiai registruojami ir apie tai informuojami EIS administratoriai ir EIS naudotojai;

21.11. EIS administratorius savo administruojamiems EIS naudotojams privalo pateikti visą reikalingą informaciją apie naudojimosi EIS pakitimus.

22. EIS naudotojai, savo darbo funkcijoms vykdyti naudojantys nešiojamuosius kompiuterius ar kitus mobiliuosius įrenginius, EIS duomenims perduoti kompiuterių ir kitų mobiliųjų įrenginių tinklais ne savo darbo vietoje privalo naudoti kompiuterio įjungimo slaptažodį ir papildomai patvirtinti EIS naudotojo tapatybę.

IV SKYRIUS
REIKALAVIMAI, KELIAMI EIS FUNKCIONAVIMUI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

23. Paslaugų teikėjų prieigos prie EIS lygiai ir sąlygos:

23.1. administratorius suteikia prieigos prie EIS duomenų teisę (peržiūrėti EIS duomenis, atlikti užklausas EIS, vykdyti veiksmus su EIS duomenimis ir kt.), fizinę prieigą prie EIS techninės ir programinės įrangos paslaugų teikėjo įgaliotam fiziniam asmeniui paslaugų teikimo sutartyje nustatytomis sąlygomis ir tvarka paslaugų teikėjo funkcijoms atlikti;

23.2. administratorius, suteikdamas prieigos prie EIS duomenų teisę, paslaugų teikėjo įgaliotą fizinį asmenį supažindina su EIS nuostatais, EIS duomenų saugos nuostatais ir kitais EIS saugos politikos įgyvendinamaisiais dokumentais;

23.3. pasibaigus paslaugų teikimo sutarties galiojimui ar šią sutartį nutraukus, administratorius nedelsdamas, bet ne vėliau kaip kitą darbo dieną, panaikina paslaugų teikėjo įgalioto fizinio asmens prieigos prie EIS duomenų teisę ir apie tai jį informuoja.

24. Reikalavimai EIS tarnybinių stočių patalpų, EIS programinės įrangos, EIS priežiūrai ir kitoms paslaugoms:

24.1. reikalavimai paslaugų teikėjams ir jų teikiamoms EIS priežiūros paslaugoms nustatomi šių paslaugų teikimo sutartyse;

24.2. paslaugų teikimo sutartyje turi būti nurodoma, kad paslaugų teikėjas kuria ar modifikuoja EIS programinę įrangą, naudodamas:

24.2.1. įgyvendintas elektroninės informacijos saugos priemones, apsaugančias nuo neteisėto poveikio sisteminei, programinei įrangai ir patalpoms;

24.2.2. EIS testinės duomenų bazės duomenis (EIS programinei įrangai modifikuoti);

24.2.3. tik sertifikuotą EIS programinę įrangą;

24.3. EIS veiklą palaikančių sistemų (elektros energijos, šildymo, vėdinimo ir oro kondicionavimo bei kitos sistemos) kokybė atsižvelgiant į šių sistemų veiklai keliamus reikalavimus turi būti reguliariai tikrinama, siekiant užtikrinti tinkamą šių paslaugų teikimą ir sumažinti galimas šių paslaugų teikimo sutrikimo ir avarijos pasekmes.

_____

PATVIRTINTA
Lietuvos automobilių kelių direkcijos prie
Susisiekimo ministerijos direktoriaus
2016 m. birželio 16 d.
įsakymu Nr. V-332

VALSTYBINĖS REIKŠMĖS KELIŲ EISMO INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės reikšmės kelių eismo informacinės sistemos veiklos tęstinumo valdymo plano (toliau – Valdymo planas) tikslas – nustatyti Valstybinės reikšmės kelių eismo informacinės sistemos (toliau – EIS) administratoriaus, EIS saugos įgaliotinio ir kitų asmenų veiksmus, įvykus elektroninės informacijos saugos incidentui, kurio metu iškyla pavojus EIS duomenims, EIS techninės, programinės įrangos funkcionavimui.

2. Valdymo planas parengtas vadovaujantis Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“, Valstybinės reikšmės kelių eismo informacinės sistemos nuostatais ir Valstybinės reikšmės kelių eismo informacinės sistemos duomenų saugos nuostatais, patvirtintais Lietuvos automobilių kelių direkcijos prie Susisiekimo ministerijos direktoriaus 2016 m. vasario 17 d. įsakymu Nr. V-126 „Dėl Valstybinės reikšmės kelių eismo informacinės sistemos nuostatų ir Valstybinės reikšmės kelių eismo informacinės sistemos duomenų saugos nuostatų patvirtinimo“.

3. Valdymo plane vartojamos sąvokos atitinka Valdymo plano 2 punkte nurodytuose teisės aktuose apibrėžtas sąvokas.

4. Valdymo plano reikalavimai privalomi EIS tvarkytojui, valdytojui, naudotojams, administratoriui, saugos įgaliotiniui, naudojantiems EIS įrangą tarnybos ir darbo funkcijoms atlikti.

5. Valdymo planas turi būti įgyvendinamas įvykus elektroninės informacijos saugos incidentui, kurio metu gali kilti pavojus EIS duomenims, EIS techninės, programinės įrangos funkcionavimui.

6. Saugos įgaliotinio, administratoriaus ir EIS duomenų tvarkytojo veiksmai įvykus elektroninės informacijos saugos incidentui yra nurodyti Detaliajame ekstremaliosios situacijos valdymo ir veiklos atkūrimo plane (Valdymo plano 1 priedas).

7. Elektroninės informacijos saugos incidento metu patirti nuostoliai padengiami iš valstybės biudžeto ir kitų finansavimo šaltinių.

8. Kriterijai, pagal kuriuos nustatoma, kad EIS veikla atkurta:

8.1. EIS duomenų atnaujinimas;

8.2. EIS duomenų išsaugojimas;

8.3. nuolatinis EIS duomenų teikimas fiziniams, juridiniams asmenims ar kitoms užsienio organizacijoms ir kitoms informacinėms sistemoms teisės aktų nustatyta tvarka.

9. Neveikiant EIS ar jai veikiant iš dalies, jos veikla turi būti atkurta per 12 valandų. Atkūrimas vykdomas pagal Valdymo plane numatytą prioritetą (valdymo plano 2 priedas

„Valstybinės reikšmės kelių eismo informacinės sistemos funkcijų atkūrimo prioritetai ir atsakomybė“).

10. EIS prieinamumas turi būti užtikrintas ne mažiau kaip 96 proc. paros laiko.

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

11. Elektroninės informacijos saugos incidentams valdyti ir veiklos atkūrimui organizuoti EIS duomenų tvarkytojo vadovo įsakymu sudaroma EIS veiklos tęstinumo valdymo grupė (toliau – Valdymo grupė) ir EIS veiklos atkūrimo grupė (toliau – Atkūrimo grupė).

12. Valdymo grupės tikslas – pagal EIS saugos įgaliotinio gautą tarnybinį pranešimą apie elektroninės informacijos saugos incidentą tirti elektroninės informacijos saugos incidentus, ieškoti priemonių ir būdų sukeltiems padariniams bei žalai likviduoti, užtikrinti EIS veiklos tęstinumą.

13. Valdymo grupės sudėtis:

13.1. EIS duomenų tvarkytojo vadovas (Valdymo grupės vadovas), kuris atsakingas už Valdymo plano 14.1, 14.3, 14.4 ir 15.6 papunkčiuose nurodytų funkcijų atlikimą;

13.2. EIS duomenų tvarkytojo EIS projektų vadovas (Valdymo grupės vadovo pavaduotojas), kuris atsakingas už Valdymo plano 14.1, 14.3, 14.4, 14.6 ir 14.8 papunkčiuose nurodytų funkcijų atlikimą;

13.3. saugos įgaliotinis, kuris atsakingas už Valdymo plano 14.1, 14.2, 14.3 ir 14.5 papunkčiuose nurodytų funkcijų atlikimą;

13.4. administratorius, kuris atsakingas už Valdymo plano 14.1, 14.2, 14.3, 14.5, 14.7 ir 15.8 papunkčiuose nurodytų funkcijų atlikimą;

13.5. kiti EIS duomenų tvarkytojo vadovo įsakymu paskirti EIS valdytojo valstybės tarnautojai arba darbuotojai, dirbantys pagal darbo sutartis, ar EIS duomenų tvarkytojo darbuotojai, dirbantys pagal darbo sutartis.

14. Valdymo grupės funkcijos:

14.1. elektroninės informacijos saugos incidentų analizė ir sprendimų EIS veiklos tęstinumo valdymo klausimais priėmimas;

14.2. bendravimas ir bendradarbiavimas su EIS naudotojais;

14.3. bendravimas ir bendradarbiavimas su teisėsaugos ir kitomis institucijomis bei kitomis interesų grupėmis;

14.4. bendravimas ir bendradarbiavimas su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;

14.5. bendravimas ir bendradarbiavimas su kitų valstybės registrų ir informacinių sistemų veiklos tęstinumo valdymo grupėmis;

14.6. finansinių ir kitų išteklių, reikalingų EIS veiklai atkurti, įvykus elektroninės informacijos saugos incidentui, naudojimo kontrolė;

14.7. EIS fizinės duomenų saugos užtikrinimo kontrolė, įvykus elektroninės informacijos saugos incidentui;

14.8. logistikos organizavimas (žmonių, daiktų, įrangos gabenimas);

14.9. EIS veiklos atkūrimo priežiūra ir koordinavimas;

14.10. kitos Valdymo grupei pavestos funkcijos.

15. Atkūrimo grupės sudėtis:

15.1. EIS duomenų tvarkytojo vadovas (Atkūrimo grupės vadovas), kuris atsakingas už Valdymo plano 16.1–16.6 papunkčiuose nurodytų funkcijų atlikimą;

15.2. saugos įgaliotinis (Atkūrimo grupės vadovo pavaduotojas), kuris atsakingas už Valdymo plano 16.1–16.6 papunkčiuose nurodytų funkcijų atlikimą;

15.3. administratorius, kuris atsakingas už Valdymo plano 16.1–16.6 papunkčiuose nurodytų funkcijų atlikimą;

15.4. EIS duomenų tvarkytojo EIS projektų vadovas, kuris atsakingas už Valdymo plano 17.1–17.6 papunkčiuose nurodytų funkcijų atlikimą;

15.5. kiti EIS duomenų tvarkytojo vadovo įsakymu paskirti EIS valdytojo valstybės tarnautojai arba darbuotojai, dirbantys pagal darbo sutartis, ar EIS duomenų tvarkytojo darbuotojai, dirbantys pagal darbo sutartis.

16. Atkūrimo grupės funkcijos:

16.1. EIS funkcionalumo atkūrimo valdymas;

16.2. EIS tarnybinių stočių veikimo atkūrimo organizavimas;

16.3. kompiuterių tinklo veikimo atkūrimo organizavimas;

16.4. EIS duomenų atkūrimo organizavimas;

16.5. EIS taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

16.6. kompiuterių veikimo atkūrimo ir prijungimo prie kompiuterių tinklo organizavimas;

16.7. kitos Atkūrimo grupei pavestos funkcijos.

17. Valdymo ir Atkūrimo grupės tarpusavyje bendrauja el. paštu ir (ar) telefonu. Ne rečiau negu kartą per metus organizuojamas šių grupių susitikimas, kuriame aptariama esama situacija ir suderinami galimi jos gerinimo būdai.

18. Įvykus elektroninės informacijos saugos incidentui:

18.1. EIS naudotojai privalo nedelsdami žodžiu ar raštu pranešti administratoriui apie elektroninės informacijos saugos incidentą; EIS naudotojai neturi teisės imtis jokių veiksmų;

18.2. administratorius nedelsdamas turi imtis atitinkamų atsakomųjų veiksmų, reikalingų elektroninės informacijos saugos incidentui stabdyti; apie elektroninės informacijos saugos incidentą administratorius, įvertinęs incidento reikšmingumą, raštu informuoja saugos įgaliotinį; įvykis aprašomas, nurodant elektroninės informacijos saugos incidento vietą, laiką, pobūdį ir kitą su įvykiu susijusią informaciją;

18.3. saugos įgaliotinis apie elektroninės informacijos saugos incidentą nedelsdamas informuoja EIS valdytojo vadovą;

18.4. saugos įgaliotinis įrašo informaciją apie elektroninės informacijos saugos incidentą į Valstybinės reikšmės kelių eismo informacinės sistemos veiklos tęstinumo elektroninės informacijos saugos incidentų registravimo žurnalą (Valdymo plano 3 priedas), vadovauja EIS veiklos atkūrimo detaliajame plane nurodytiems veiksmams;

18.5. administratorius atkuria EIS techninės ir programinės įrangos veikimą, kompiuterių tinklo veiklą, EIS duomenis, EIS techninės, sisteminės ir taikomosios programinės įrangos funkcionavimą ir nedelsdamas informuoja saugos įgaliotinį;

18.6. saugos įgaliotinis kartu su administratoriumi organizuoja žalos, padarytos EIS duomenims, EIS techninei, programinei įrangai, vertinimą, koordinuoja EIS veiklai atkurti reikalingos techninės, sisteminės ir taikomosios programinės įrangos įsigijimą;

18.7. elektroninės informacijos saugumo incidentui išplitus už EIS valdytojo ir EIS duomenų tvarkytojo įstaigos ribų, administratorius informuoja su elektroninės informacijos saugos incidentu susijusius paslaugų teikėjus ir (ar) kitas institucijas, atsižvelgia į jų rekomendacijas.

19. Techninė, sisteminė ir taikomoji programinė įranga, reikalinga elektroninės informacijos saugos incidento metu sunaikintai ar sugadintai įrangai pakeisti, įsigyjama Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka.

20. Atsarginėms patalpoms, naudojamoms EIS veiklai atkurti elektroninės informacijos saugos incidento atveju, keliami šie reikalavimai:

20.1. patekimas į atsargines patalpas turi būti registruojamas patekimo į patalpas, kuriose yra tarnybinės stotys, žurnale;

20.2. atsarginės patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų;

20.3. atsarginės patalpos turi atitikti gaisrinės saugos reikalavimus ir jose turi būti pirminių gaisro gesinimo priemonių;

20.4. atsarginėse patalpose turi būti įrengtas rezervinis elektros energijos šaltinis EIS techninei įrangai ir duomenų perdavimo tinklo mazgams, užtikrinantis nurodytos įrangos veikimą pagrindinio elektros energijos šaltinio neveikimo atveju ne trumpiau kaip 30 min.;

20.5. ryšių kabeliai turi būti apsaugoti nuo nesankcionuoto prisijungimo;

20.6. patalpoje nuolat turi veikti oro temperatūros reguliavimo įranga (oro kondicionavimo sistema) ir turėtų būti palaikoma +22 (±5) ºC temperatūra.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

21. EIS veiklos tęstinumo vykdymo užtikrinimui turi būti surinkta ir naudojama detali bei aktuali informacija, būtina EIS veiklai atkurti.

22. Už EIS veiklos tęstinumo vykdymui reikalingos detaliosios informacijos rengimą, atnaujinimą ir saugojimą atsakingas administratorius.

23. Detalią informaciją sudaro:

23.1. dokumentas, kuriame nurodyti informacinių technologijų įrangos parametrai ir už šios įrangos priežiūrą atsakingas (-i) administratorius (-iai), minimalus EIS veiklai atkurti nesant administratoriaus, kuris dėl komandiruotės, ligos ar kitų priežasčių negali operatyviai atvykti į darbo vietą, reikiamos kompetencijos ar žinių lygis;

23.2. dokumentas, kuriame nurodyta minimalaus funkcionalumo informacinių technologijų įrangos, tinkamos institucijos poreikius atitinkančiai EIS veiklai užtikrinti įvykus elektroninės informacijos saugos incidentui, specifikacija;

23.3. dokumentas, kuriame nurodyti kiekvieno pastato, kuriame yra informacinės sistemos įranga, aukšto patalpų brėžiniai ir juose pažymėti:

23.3.1. tarnybinės stotys;

23.3.2. kompiuterio tinklo ir telefonų tinklo mazgai;

23.3.3. kompiuterių tinklo ir telefonų tinklo laidų vedimo tarp pastato aukštų vietos;

23.3.4. elektros tinklo įvado pastate vietos;

23.4. dokumentas, kuriame nurodytos kompiuterių tinklo fizinio ir loginio sujungimo schemos;

23.5. dokumentas, kuriame nurodytos atsarginių laikmenų su programinėmis įrangos kopijomis saugojimo taisyklės, elektroninės informacijos teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutartys, atsakingų už šių sutarčių įgyvendinimo priežiūrą asmenų pareigos;

23.6. dokumentas, kuriame nurodyta programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos;

23.7. dokumentas, kuriame nurodytas veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės narių sąrašas su kontaktiniais duomenimis, leidžiančiais pasiekti šiuos asmenis bet kuriuo metu.

IV SKYRIUS
VALDYMO PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

24. Valdymo plano veiksmingumas turi būti išbandomas kartą per metus. Valdymo plano veiksmingumo išbandymo metu imituojamas elektroninės informacijos saugos incidentas. Jo metu už elektroninės informacijos saugos incidento padarinių likvidavimą atsakingi asmenys atlieka minėtų padarinių likvidavimo veiksmus. Iš atsarginių EIS duomenų kopijų atkuriami EIS duomenys.

25. Pagal bandymų rezultatus saugos įgaliotinis ir administratorius parengia EIS veiklos tęstinumo valdymo plano bandymų ataskaitą (toliau – ataskaita) (Valdymo plano 4 priedas), kurioje yra apibendrinami atliktų bandymų rezultatai, apibrėžiami pastebėti trūkumai ir pasiūlomos šių trūkumų šalinimo priemonės. Ataskaitą įvertina EIS duomenų tvarkytojo informacinių sistemų projektų priežiūros komitetas ir priima sprendimus dėl trūkumų šalinimo. Informacinių sistemų projektų priežiūros komiteto sudėtis ir darbo reglamentas patvirtinami EIS duomenų tvarkytojo vadovo įsakymu.

26. Saugos įgaliotinis nuolat kontroliuoja ataskaitoje nurodytų trūkumų šalinimo priemonių įgyvendinimą.

27. Valdymo plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami laikantis šių principų:

27.1. operatyvumo – kiek galima greičiau išspręsti ir pašalinti trūkumus. Atliekant trūkumų šalinimo veiklą, turi būti atsižvelgiama į trūkumų sudėtingumą ir apimtį. Saugos įgaliotinis kartu su administratoriumi nusprendžia ir nustato, per kiek laiko turi būti atliktas konkretus trūkumų šalinimo veiksmas ir pašalinti trūkumai;

27.2. veiksmingumo – trūkumų šalinimas turi padaryti esminę įtaką EIS veiklai; trūkumų šalinimas laikomas veiksmingu, jei jo metu pavyko sumažinti konkretaus trūkumo neigiamą poveikį;

27.3. ekonomiškumo – siekis taupiai naudojant turimus išteklius pašalinti visus trūkumus.

_____