LIETUVOS AUTOMOBILIŲ KELIŲ DIREKCIJOS PRIE SUSISIEKIMO MINISTERIJOS DIREKTORIUS

ĮSAKYMAS DĖL LIETUVOS AUTOMOBILIŲ KELIŲ DIREKCIJOS PRIE SUSISIEKIMO MINISTERIJOS GENERALINIO DIREKTORIAUS 2007 M. LIEPOS 17 D. ĮSAKYMO NR. V-188 „DĖL LIETUVOS AUTOMOBILIŲ KELIŲ DIREKCIJOS PRIE SUSISIEKIMO MINISTERIJOS INFORMACINĖS SISTEMOS „KELIŲ PROJEKTAI“ DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO

2015 m. birželio 25 d. Nr. V(E)-13
Vilnius

1. P a k e i č i u Lietuvos automobilių kelių direkcijos prie Susisiekimo ministerijos generalinio direktoriaus 2007 m. liepos 17 d. įsakymą Nr. V-188 „Dėl Lietuvos automobilių kelių direkcijos prie Susisiekimo ministerijos informacinės sistemos „Kelių projektai“ duomenų saugos nuostatų patvirtinimo“ ir išdėstau jį nauja redakcija:

„LIETUVOS AUTOMOBILIŲ KELIŲ DIREKCIJOS PRIE SUSISIEKIMO MINISTERIJOS DIREKTORIUS

ĮSAKYMAS DĖL INFORMACINĖS SISTEMOS „KELIŲ PROJEKTAI“ DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

Vadovaudamasis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimo aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 7.1 ir 11 punktais,

t v i r t i n u Informacinės sistemos „Kelių projektai“ duomenų saugos nuostatus (pridedama).“

2. P a v e d u per 5 mėnesius nuo šio įsakymo įsigaliojimo Informacinių technologijų skyriaus patarėjai Tatjanai Kržečkovskajai parengti informacinės sistemos „Kelių projektai“ saugaus elektroninės informacijos tvarkymo taisyklių, informacinės sistemos „Kelių projektai“ veiklos tęstinumo valdymo plano ir informacinės sistemos „Kelių projektai“ naudotojų administravimo taisyklių naują redakciją.

Direktoriaus pavaduotojas,
laikinai einantis direktoriaus pareigas Dainius Miškinis

SUDERINTA

Lietuvos Respublikos vidaus reikalų ministerijos

2015 m. gegužės 19 d. raštu Nr. 1(E)-43

PATVIRTINTA
Lietuvos automobilių kelių direkcijos
prie Susisiekimo ministerijos
generalinio direktoriaus
2007 m. liepos 17 d. įsakymu Nr. V-188
(Lietuvos automobilių kelių direkcijos
prie Susisiekimo ministerijos direktoriaus
2015 m. birželio 25 d. įsakymo Nr. V(E)-13
redakcija)

INFORMACINĖS SISTEMOS „KELIŲ PROJEKTAI“ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Informacinės sistemos „Kelių projektai“ duomenų saugos nuostatai (toliau – saugos nuostatai) reglamentuoja informacinės sistemos „Kelių projektai“ (toliau – IS KP) saugos politiką ir administracines, technines ir kitas priemones, kurios užtikrina saugų ir teisėtą IS KP duomenų tvarkymą.

2. IS KP elektroninės informacijos saugumo užtikrinimo tikslas – sudaryti sąlygas saugiai automatizuotai tvarkyti IS KP elektroninius duomenis, išsaugant jų konfidencialumą, vientisumą ir prieinamumą.

3. Siekiant užtikrinti saugų IS KP veikimą, nustatomos elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

3.1. administracinių, techninių ir kitų priemonių, skirtų duomenų saugai užtikrinti, įgyvendinimas ir kontrolė;

3.2. veiklos tęstinumo užtikrinimas.

4. Saugos nuostatuose vartojamos sąvokos atitinka saugos nuostatų 9 punkte nurodytuose teisės aktuose vartojamas sąvokas.

5. IS KP valdytojas ir tvarkytojas yra Lietuvos automobilių kelių direkcija prie Susisiekimo ministerijos (toliau – Kelių direkcija) (J. Basanavičiaus g. 36, LT-03109 Vilnius).

6. IS KP valdytojo ir tvarkytojo funkcijos:

6.1. atlikti saugos reikalavimų laikymosi priežiūrą;

6.2. tvirtinti teisės aktus, susijusius su duomenų tvarkymu ir duomenų sauga;

6.3. tvirtinti IS KP saugos reikalavimus;

6.4. atsakyti už elektroninių duomenų saugų tvarkymą;

6.5. kontroliuoti, kaip laikomasi saugos reikalavimų;

6.6. užtikrinti eksploataciją ir veikimo priežiūrą, įgyvendinti pokyčius ir tolesnę plėtrą, prižiūrėti techninę ir programinę įrangą, planuoti atnaujinimus ir pajėgumus;

6.7. užtikrinti IS KP veiklos tęstinumą ir veiklos atkūrimą, šalinti sutrikimus;

6.8. sukurti automatinių duomenų mainų su duomenų teikėjais ir gavėjais sąsajas ir vykdyti jų priežiūrą;

6.9. gauti duomenis iš kitų informacinių sistemų, teikti informaciją registrams ir kitoms informacinėms sistemoms;

6.10. skirti IS KP administratorių;

6.11. analizuoti IS KP procesus ir IS KP naudotojų veiksmus;

6.12. vykdyti kitas saugos nuostatuose ir kituose teisės aktuose nurodytas funkcijas.

7. Saugos įgaliotinio funkcijos:

7.1. teikti IS KP valdytojo ir tvarkytojo vadovui pasiūlymus dėl:

7.1.1. IS KP administratoriaus (administratorių) paskyrimo ir reikalavimų administratoriui (administratoriams) nustatymo;

7.1.2. IS KP saugos dokumentų priėmimo ir keitimo;

7.1.3. IS KP saugos reikalavimų atitikties vertinimo atlikimo;

7.2. koordinuoti elektroninės informacijos saugos incidentų, įvykusių IS KP, tyrimą ir bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės;

7.3. teikti administratoriui (administratoriams) ir IS KP naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;

7.4. ne rečiau kaip kartą per metus, jeigu teisės aktai nenustato kitaip, organizuoti IS KP rizikos įvertinimą;

7.5. periodiškai organizuoti IS KP naudotojų mokymą elektroninės informacijos saugos klausimais, įvairiais būdais informuoti juos apie elektroninės informacijos saugos problemas (priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės naujiems darbuotojams ir kt.);

7.6. vykdyti kitų su elektroninės informacijos sauga susijusių teisės aktų nustatytas ir IS KP valdytojo pavestas funkcijas.

8. IS KP administratoriaus funkcijos:

8.1. kontroliuoti IS KP veikimą;

8.2. registruoti IS KP naudotojus sistemoje, tvarkyti jų duomenis, prieigos teises ir leidžiamus IS KP veiksmus;

8.3. dalyvauti svarstant teikimus dėl IS KP pokyčių projektavimo, konstravimo ir diegimo, dalyvauti aptariant IS KP plėtrą ir vykdant IS KP plėtros specifikavimo, projektavimo, konstravimo ir diegimo etapų darbus;

8.4. organizuoti IS KP konfigūravimą, įskaitant saugų IS KP įjungimą ir išjungimą;

8.5. užtikrinti nepertraukiamą IS KP veikimą;

8.6. reguliuoti techninių išteklių naudojimą;

8.7. diegti ir atnaujinti IS KP programinę įrangą;

8.8. konsultuoti IS KP naudotojus;

8.9. spręsti iškilusias problemas ir apie jas informuoti saugos įgaliotinį ir IS KP tvarkytoją;

8.10. teikti saugos įgaliotiniui pasiūlymus dėl IS KP saugos organizavimo, vykdyti kitas saugos nuostatų ir kitų informacinių sistemų saugą reglamentuojančių teisės aktų nustatytas funkcijas;

8.11. vykdyti IS KP tvarkytojo ir (ar) saugos įgaliotinio pavestas funkcijas.

9. Tvarkant IS KP elektroninius duomenis ir užtikrinant saugą vadovaujamasi šiais teisės aktais:

9.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

9.2. Lietuvos Respublikos kibernetinio saugumo įstatymu;

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

9.4. Lietuvos standartais LST ISO/IEC 27002:2014 ir LST ISO/IEC 27001:2013, kitais Lietuvos Respublikos ir tarptautiniais grupės „Informacijos technologija. Saugumo metodai“ standartais, naudojamais kaip elektroninės informacijos saugos užtikrinimo rekomendacinės priemonės;

9.5. 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. IV-832 (toliau – techniniai reikalavimai);

9.6. kitais teisės aktais ir dokumentais, reglamentuojančiais informacinių sistemų duomenų tvarkymo teisėtumą ir elektroninių duomenų saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

10. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 4.3.2 ir 4.3.4 punktais, IS KP tvarkoma elektroninė informacija priskiriama žinybinės svarbos elektroninės informacijos kategorijai.

11. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 5.2 punktu, IS KP priskiriama trečios kategorijos informacinėms sistemoms.

12. IS KP elektroninius duomenis tvarkyti gali tik tie IS KP naudotojai, kurie yra susipažinę su IS KP nuostatais, saugos nuostatais ir kitais saugos dokumentais.

13. IS KP rizikos įvertinimas atliekamas vadovaujantis šiomis nuostatomis:

13.1. rizikos įvertinimas atliekamas ne rečiau kaip kartą per metus, jeigu teisės aktai nenustato kitaip. Prireikus saugos įgaliotinis gali organizuoti neeilinį IS KP rizikos įvertinimą. Neeilinis rizikos vertinimas atliekamas pasikeitus IS KP struktūrai (esminiai IS KP funkciniai pakitimai ir programinės įrangos keitimas), įvykus dideliems Kelių direkcijos organizaciniams pokyčiams, atsiradus naujų informacinių technologijų saugos srities reikalavimų, po didelio masto saugos incidentų ir nustačius naujų rizikos formų;

13.2. atliekant rizikos įvertinimą, rekomenduojama vadovautis Lietuvos standartais LST ISO/IEC 27002:2014 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ ir LST ISO/IEC 27001:2013 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“ ar naujesniais tarptautiniais standartais, geriausios praktikos pavyzdžiais (COBIT ar kitais) ir elektroninės informacijos saugą reglamentuojančiais teisės aktais;

13.3. rizikos įvertinimui atlikti sutartiniais pagrindais gali būti samdomi tretieji asmenys.

14. IS KP rizikos įvertinimas išdėstomas rizikos įvertinimo ataskaitoje. IS KP rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos IS KP elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. IS KP rizikos įvertinimo ataskaitą rengia arba, jei vertinimą atlieka trečioji šalis, dalyvauja rengiant saugos įgaliotinis.

15. Svarbiausieji rizikos veiksniai:

15.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);

15.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis siekiant gauti IS KP elektroninę informaciją, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymas, saugos pažeidimai, vagystės ir kita);

15.3. nenugalima jėga (*force majeure*).

16. Atsižvelgdamas į rizikos įvertinimo ataskaitą, IS KP valdytojas prireikus tvirtina IS KP rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

17. Siekdamas užtikrinti saugos nuostatuose ir kituose saugos politikos įgyvendinamuosiuose teisės aktuose išdėstytų nuostatų įgyvendinimo kontrolę, saugos įgaliotinis ne rečiau kaip kartą per metus atlieka IS KP informacinių technologijų saugos atitikties vertinimą.

18. Atlikus IS KP informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita ir prireikus pastebėtų trūkumų šalinimo planas, kurį tvirtina, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminus IS KP valdytojo vadovas.

19. Pagrindiniai elektroninės informacijos saugos priemonių parinkimo principai:

19.1. parenkamos priemonės, kurios leidžia užtikrinti patalpų saugą;

19.2. parenkamos priemonės, kurios leidžia užtikrinti kompiuterinės ir programinės įrangos veikimo saugą;

19.3. parenkamos priemonės, kurios leidžia užtikrinti kompiuterių tinklų veikimo saugą;

19.4. parenkamos priemonės, kurios leidžia užtikrinti IS KP naudotojų mokymą ir informavimą apie elektroninių duomenų tvarkymo saugą.

20. Elektroninės informacijos saugos priemonės turi garantuoti:

20.1. elektroninių duomenų saugą jų registravimo ir perdavimo ryšio kanalais, saugojimo, apdorojimo, teikimo ir naudojimo metu;

20.2. elektroninių duomenų saugą nuo nesankcionuoto ar neteisėto naudojimo, kaupimo, keitimo, perdavimo, skelbimo ir sunaikinimo;

20.3. elektroninių duomenų saugą nuo jų pažeidimo esant šiems rizikos veiksniams:

20.3.1. subjektyviems netyčiniams vidiniams ir išoriniams veiksniams;

20.3.2. subjektyviems tyčiniams vidiniams ir išoriniams veiksniams;

20.3.3. esant nenugalimai jėgai (*force majeure*).

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

21. Programinės įrangos, kuri užtikrina saugų IS KP veikimą, naudojimo nuostatos ir reikalavimai:

21.1. IS KP turi būti naudojama tik legali programinė įranga;

21.2. programinės įrangos diegimą turi atlikti tik įgalioti asmenys;

21.3. Kelių direkcijos tarnybinėse stotyse ir IS KP naudotojų kompiuterizuotose darbo vietose privalo būti naudojama programinė įranga, kuri apsaugo nuo kenksmingos programinės įrangos ir kuri turi būti atnaujinama ne rečiau kaip kartą per parą;

21.4. turi būti naudojama programinė įranga, leidžianti atlikti IS KP naudojamų kompiuterių tinklų stebėseną ir užtikrinanti šių tinklų saugos prevencines priemones.

22. Prieigos prie IS KP užtikrinimo priemonės:

22.1. už IS KP naudotojų teisių suteikimą atsako IS KP administratorius;

22.2. tiesioginė prieiga prie IS KP suteikiama naudojant IS KP naudotojų identifikavimo priemones;

22.3. turi būti realizuota prievolė periodiškai keisti slaptažodžius;

22.4. IS KP naudotojams užtikrinamas ne mažesnis kaip 90 proc. IS KP prieinamumas darbo laiko metu.

23. Kompiuterizuotų darbo vietų, kuriose veikia IS KP, saugaus naudojimo nuostatos ir reikalavimai:

23.1. stacionariuosiuose ir nešiojamuosiuose kompiuteriuose IS KP įjungimo metu turi būti identifikuojamas IS KP naudotojas;

23.2. Kelių direkcijos IS KP naudotojų kompiuterizuotose darbo vietose draudžiama naudoti programinę įrangą, nesusijusią su tiesiogine jų veikla ir funkcijomis;

23.3. kompiuterizuotos darbo vietos, programinė įranga, jos sertifikatai ir licencijos kasmet turi būti inventorizuojami;

23.4. IS KP naudotojų nešiojamieji kompiuteriai ne institucijos patalpose privalo būti naudojami tik su tiesioginių pareigų atlikimu susijusiai veiklai atlikti;

23.5. už saugų IS KP kompiuterių tinklų veikimą pagal kompetenciją atsako IS KP tvarkytojo kompiuterių tinklų administratoriai.

24. Saugaus elektroninės informacijos teikimo ir gavimo metodai:

24.1. užtikrinant saugų elektroninės informacijos keitimąsi su kitomis valstybės institucijomis ir savivaldybėmis privaloma naudotis saugiu duomenų perdavimo protokolu *https* ir ne ilgiau kaip vienerius metus galiojančiu prisijungimo sertifikatu;

24.2. duomenų gavėjų prieigą prie IS KP kontroliuoja kompiuterių tinklo užkarda.

25. Nustatomi šie pagrindiniai atsarginių elektroninių duomenų kopijų (toliau – atsarginės kopijos) darymo ir atkūrimo reikalavimai:

25.1. atsarginės kopijos turi būti daromos automatiškai kiekvieną dieną;

25.2. už atsarginės kopijų darymą yra atsakingas IS KP administratorius;

25.3. atsarginės kopijos įrašomos į keičiamus informacijos kaupiklius (juostas, kompaktinius diskus ir pan.) ir saugomos sistemos administratoriaus, o jo nesant – administratorių pavaduojančio asmens;

25.4. atsarginės kopijos turi būti saugomos kitose patalpose, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate;

25.5. atkūrimo iš atsarginės kopijų galimybė privalo būti patikrinama ne rečiau kaip kartą per metus;

25.6. turi būti užtikrinta IS KP pagrindinių funkcijų atkūrimo per 16 val. nuo veiklos sutrikimo galimybė.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

26. Saugos įgaliotinis privalo išmanyti šiuolaikinių informacinių technologijų naudojimo ypatumus, elektroninės informacijos saugos principus ir saugos užtikrinimo metodus, kitus su informacinių sistemų saugiu veikimu susijusius teisės aktus ir gebėti organizuoti darbą.

27. Saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumo srityje, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėjo mažiau nei vieneri metai.

28. IS KP administratorius privalo gerai išmanyti veiklos procesus, elektroninės informacijos saugos užtikrinimo metodus ir principus, tarnybinių stočių veikimo principus, būti susipažinęs su naudojamų duomenų bazių organizavimo principais ir gebėti jas administruoti.

29. IS KP naudotojai privalo turėti pagrindinių darbo su kompiuteriu įgūdžių, mokėti tvarkyti duomenis, gilinti kompiuterines žinias ir būti susipažinę su IS KP duomenų saugos politiką įgyvendinančiais dokumentais.

30. IS KP naudotojai turi būti mokomi dirbti su IS KP. Mokymus, esant poreikiui, organizuoja IS KP tvarkytojas.

31. Elektroninės informacijos saugos mokymai IS KP administratoriui ir IS KP naudotojams turi būti rengiami ne rečiau kaip vieną kartą per metus.

V SKYRIUS
IS KP NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

32. IS KP administratorius ir IS KP naudotojai turi būti susipažinę su saugos nuostatais ir kitais elektroninės informacijos saugą reglamentuojančiais teisės aktais bei atsakomybe už šių reikalavimų nesilaikymą.

33. IS KP administratoriaus, IS KP naudotojų supažindinimą su saugos nuostatais, kitais elektroninės informacijos saugą reglamentuojančiais teisės aktais organizuoja saugos įgaliotinis. Saugos įgaliotinis raštu ir elektroniniu paštu informuoja IS KP tvarkytoją, IS KP administratorių ir IS KP naudotojus apie saugos nuostatų ir kitų elektroninės informacijos saugą reglamentuojančių teisės aktų pasikeitimus ar jų negaliojimą, naujų teisės aktų priėmimą.

34. Saugos nuostatai ir kiti saugos politikos įgyvendinamieji teisės aktai skelbiami IS KP naudotojams pasiekiamoje interneto svetainėje.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

35. Saugos nuostatai, kiti IS KP tvarkomos elektroninės informacijos saugą reglamentuojantys teisės aktai ir kiti dokumentai iš esmės peržiūrimi ne rečiau kaip kartą per metus ir prireikus keičiami.

36. Saugos įgaliotinis, IS KP administratorius ir IS KP naudotojai, pažeidę saugos nuostatų ar kitų saugos politiką reglamentuojančių teisės aktų reikalavimus, atsako įstatymų nustatyta tvarka.

_____