Suvestinė redakcija nuo 2016-05-13 iki 2020-10-28

Įsakymas paskelbtas: Žin. 2011, Nr. 25-1246, i. k. 1112214ISAK0000V-73

Nauja redakcija nuo 2016-05-13:
Nr. VE-66, 2016-05-11, paskelbta TAR 2016-05-12, i. k. 2016-12505

VALSTYBINĖS GELEŽINKELIO INSPEKCIJOS
PRIE SUSISIEKIMO MINISTERIJOS
VIRŠININKAS

ĮSAKYMAS
DĖL GELEŽINKELIŲ TRANSPORTO VALSTYBINĖS PRIEŽIŪROS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2011 m. vasario 19 d. Nr. V-73
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų, patvirtintų 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“ 6.1 ir 8 punktais:

1. T v i r t i n u Geležinkelių transporto valstybinės priežiūros informacinės sistemos duomenų saugos nuostatus (pridedama);

2. S k i r i u Geležinkelių transporto valstybinės priežiūros informacinės sistemos saugos įgaliotiniu Valstybinės geležinkelio inspekcijos prie Susisiekimo ministerijos Administracinių paslaugų skyriaus vyriausiąjį specialistą Igną Bernacką.

VIRŠININKAS STASYS PIESLIKAS

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2011 m. vasario 2 d. raštu Nr. 1D-893

PATVIRTINTA
Valstybinės geležinkelio inspekcijos prie
Susisiekimo ministerijos viršininko
2011 m. vasario 19 d. įsakymu Nr. V-73
(Valstybinės geležinkelio inspekcijos prie
Susisiekimo ministerijos viršininko
2016 m. gegužės 11 d. įsakymo
Nr. VE-66 redakcija)

GELEŽINKELIŲ TRANSPORTO VALSTYBINĖS PRIEŽIŪROS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Geležinkelių transporto valstybinės priežiūros informacinės sistemos (toliau – VGI IS) duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja VGI IS saugos valdymą, organizacinius ir techninius reikalavimus, reikalavimus personalui ir VGI IS naudotojų supažindinimo su saugos dokumentais principus.

2. Saugos nuostatų tikslas – sudaryti sąlygas saugiai, automatiniu būdu tvarkyti elektroninę informaciją VGI IS, užtikrinti elektroninės informacijos konfidencialumą, prieinamumą, vientisumą ir tinkamą kompiuterizuotų darbo vietų bei tinklo įrangos funkcionavimą.

3. Saugos nuostatai parengti vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas), Saugos dokumentų turinio gairių aprašu (toliau – Saugos dokumentų turinio gairių aprašas), Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašu (toliau – Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas), 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“, 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“ ir Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu.

4. Saugos nuostatuose vartojamos sąvokos atitinka Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Lietuvos Respublikos įstatymuose ir kituose teisės aktuose bei Lietuvos standartuose LST ISO/IEC 27002:2014 ir LST ISO/IEC 27001:2013 vartojamas sąvokas.

5. Saugos nuostatų reikalavimai taikomi tvarkant VGI IS duomenis ir yra privalomi Valstybinės geležinkelio inspekcijos prie Susisiekimo ministerijos (toliau – VGI) valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartis, turintiems bet kokias VGI IS naudotojų teises.

6. Saugos nuostatai reglamentuoja VGI IS saugos politiką (toliau – Saugos politika), kurią įgyvendina šie VGI patvirtinti teisės aktai (toliau – Saugos dokumentai):

6.1. Saugaus elektroninės informacijos tvarkymo taisyklės;

6.2. Naudotojų administravimo taisyklės;

6.3. Veiklos tęstinumo valdymo planas.

7. VGI IS elektroninės informacijos saugos tikslai yra šie:

7.1. sudaryti sąlygas automatiniu būdu saugiai tvarkyti elektroninę informaciją;

7.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo ar neteisėto jos tvarkymo.

8. Elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

8.1. elektroninės informacijos prieinamumo užtikrinimas;

8.2. elektroninės informacijos vientisumo užtikrinimas;

8.3. elektroninės informacijos konfidencialumo užtikrinimas;

8.4. veiklos tęstinumo užtikrinimas.

9. VGI IS valdytojas ir tvarkytojas yra VGI, adresas: Pamėnkalnio g. 26, LT-0810, Vilnius.

10. Už VGI IS elektroninės informacijos tvarkymo teisėtumą, patikimumą, elektroninės informacijos teikimo VGI IS elektroninės informacijos gavėjams teisėtumą, patikimumą ir elektroninės informacijos saugą atsako VGI IS valdytojas.

11. VGI IS valdytojo ir tvarkytojo funkcijos ir atsakomybė:

11.1. tvirtina Saugos nuostatus, Saugaus elektroninės informacijos tvarkymo taisykles, Naudotojų administravimo taisykles, Veiklos tęstinumo valdymo planą;

11.2. prižiūri Saugos dokumentų parengimą ir įgyvendinimą;

11.3. atsižvelgdamas į rizikos įvertinimo ataskaitą, prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą;

11.4. skiria VGI IS saugos įgaliotinį (toliau – Saugos įgaliotinis);

11.5. skiria VGI IS administratorių, paveda jam užtikrinti VGI IS tarnybinių stočių saugų funkcionavimą, administruoti VGI IS duomenų bazę šių Saugos nuostatų ir kitų saugos politiką reglamentuojančių teisės aktų nustatyta tvarka;

11.6. atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi šiuose Saugos nuostatuose, Saugaus elektroninės informacijos tvarkymo taisyklėse, Naudotojų administravimo taisyklėse, Veiklos tęstinumo valdymo plane nustatyta tvarka.

12. Saugos įgaliotinis, įgyvendindamas Saugos politiką, atlieka šias funkcijas:

12.1. registruoja elektroninės informacijos saugos incidentus VGI IS elektroninės informacijos saugos incidentų registravimo žurnale, pateiktame Geležinkelių transporto valstybinės priežiūros informacinės sistemos veiklos tęstinumo valdymo plano priede Nr. 2;

12.2. koordinuoja elektroninės informacijos saugos incidentų, įvykusių VGI IS, tyrimą;

12.3. teikia VGI IS administratoriui su VGI IS elektroninės informacijos saugos užtikrinimu susijusius privalomus vykdyti nurodymus ir pavedimus;

12.4. kasmet organizuoja VGI IS rizikos vertinimą, VGI IS rizikos vertinimo rezultatai aprašomi rengiant VGI IS rizikos įvertinimo ataskaitą;

12.5. prireikus organizuoja neeilinį VGI IS rizikos vertinimą;

12.6. atlieka VGI IS informacijos saugos atitikties vertinimą;

12.7. periodiškai organizuoja VGI IS naudotojų mokymus informacijos saugos klausimais;

12.8. teikia VGI viršininkui pasiūlymus dėl:

12.8.1. VGI IS administratoriaus paskyrimo;

12.8.2. Saugos nuostatų ir Saugos dokumentų keitimo;

12.9. atlieka kitas VGI viršininko pavestas užduotis ir Bendrųjų elektroninės informacijos saugos reikalavimų apraše, jam priskirtas funkcijas;

12.10. atlieka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 8 straipsnyje numatytas duomenų valdymo įgaliotinio funkcijas.

13. VGI IS administratorius, vykdantis VGI IS priežiūrą, atlieka šias funkcijas:

13.1. vertina VGI IS naudotojų pasirengimą dirbti su VGI IS;

13.2. atlieka VGI IS naudotojams suteiktų teisių ir priskirtų funkcijų atitikties vertinimą;

13.3. rengia ir tikrina VGI IS sudarančių komponentų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, informacijos perdavimo tinklų) sąranką, nustato pažeidžiamas vietas ir saugos reikalavimų atitiktį, vykdo stebėseną;

13.4. informuoja Saugos įgaliotinį apie Saugos politikos pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias elektroninės informacijos saugos užtikrinimo priemones;

13.5. vykdo Saugos įgaliotinio nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu;

13.6. ne rečiau kaip kartą per metus ir (arba) po VGI IS pokyčio patikrina VGI IS komponentų sąranką ir VGI IS būsenos rodiklius;

13.7. nustato VGI IS pažeidžiamas vietas ir informuoja apie jas Saugos įgaliotinį;

13.8. užtikrina VGI IS duomenų saugumą ir konfidencialumą;

13.9. atlieka VGI IS techninės ir programinės įrangos priežiūrą;

13.10. atlieka VGI IS duomenų atsarginių kopijų darymą.

14. Teisės aktai, kuriais vadovaujamasi tvarkant VGI IS elektroninę informaciją ir užtikrinant jos saugumą:

14.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

14.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

14.3. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

14.4. Saugos dokumentų turinio gairių aprašas;

14.5. Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas;

14.6. 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";

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

14.8. Geležinkelių transporto valstybinės priežiūros informacinės sistemos nuostatai, patvirtinti Valstybinės geležinkelio inspekcijos prie Susisiekimo ministerijos viršininko 2011 m. vasario 17 d. įsakymu Nr. V-57 „Dėl Geležinkelių transporto valstybinės priežiūros informacinės sistemos nuostatų patvirtinimo";

14.9. Saugos dokumentai;

14.10. Lietuvos standartai LST ISO/IEC 27002:2014 ir LST ISO/IEC 27001:2013, Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo technika" grupės standartai, reguliuojantys saugų VGI IS duomenų tvarkymą;

14.11. kiti teisės aktai, reglamentuojantys Saugumo politiką ir elektroninės informacijos tvarkymo teisėtumą, valstybės informacinių sistemų tvarkytojų veiklą bei elektroninės informacijos saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

15. VGI IS tvarkoma elektroninė informacija priskirtina svarbios elektroninės informacijos kategorijai, vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 4.2.4 ir 4.2.7 papunkčių nuostatomis.

16. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 5.2 punktu, VGI IS priskiriama antrai informacinių sistemų kategorijai.

17. Saugos įgaliotinis, vadovaudamasis Lietuvos Respublikos vidaus reikalų ministerijos išleista metodine priemone „Rizikos analizės vadovas“ (http://www.vrm.lt/Rizikos_analize.pdf), Lietuvos standartu LST ISO/IEC 27005 „Informacijos technologija. Saugumo technika. Informacijos saugumo rizikos valdymas“, kasmet organizuoja VGI IS rizikos veiksnių vertinimą. Prireikus Saugos įgaliotinis gali organizuoti neeilinį VGI IS rizikos veiksnių vertinimą.

18. VGI IS rizikos įvertinimas pateikiamas rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausieji rizikos veiksniai yra šie:

18.1. subjektyvūs netyčiniai (duomenų tvarkymo klaidos ir apsirikimai, duomenų ištrynimas, klaidingas duomenų teikimas, fiziniai informacijos technologijų sutrikimai, duomenų perdavimo tinklų sutrikimai, programinės įrangos klaidos, netinkamas veikimas ir kita);

18.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema duomenims gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

18.3. nenugalima jėga (*force majeure*).

19. Rizikos veiksniai vertinami, nustatant jų galimą pasireiškimo dažnį (žemas – gali pasireikšti ne dažniau kaip 1 kartą per metus, vidutinis – gali pasireikšti ne dažniau kaip 1 kartą per 3 mėnesius, aukštas – gali pasireikšti dažniau nei 1 kartą per 3 mėnesius) ir įtakos VGI IS elektroninės informacijos saugai laipsnius:

19.1. Ž – žemas. Duomenų pažeidimo poveikio laipsnis nėra didelis, padariniai nebus pavojingi – dingo ar yra sugadinta mažesnė nei 5 proc. dalis informacijos, tačiau ją VGI IS priemonėmis galima atstatyti iš atsarginių kopijų; atskleista iki 5 proc. neviešos informacijos; VGI IS neprieinama ne daugiau nei 20 min. per parą;

19.2. V – vidutinis. Duomenų pažeidimo poveikio laipsnis gali būti didelis, padariniai rimti – dingo ar yra sugadinta mažesnė nei 50 proc. dalis informacijos, tačiau ją VGI IS priemonėmis galima atstatyti iš atsarginių kopijų; atskleista 5–20 proc. neviešos informacijos; VGI IS neprieinama ne daugiau nei 60 min. per parą;

19.3. A – aukštas. Duomenų pažeidimo poveikio laipsnis labai didelis, padariniai rimti – dingo ar yra sugadinta didesnė nei 50 proc. dalis informacijos ir (arba) dalis dingusios ar sugadintos informacijos VGI IS priemonėmis negali būti atstatyta iš atsarginių kopijų; atskleista daugiau kaip 20 proc. neviešos informacijos; VGI IS neprieinama daugiau nei 60 min. per parą.

20. Rizikos vertinimo metu atliekamos veiklos:

20.1. VGI IS sudarančių informacinių išteklių inventorizacija;

20.2. įtakos VGI IS veiklai vertinimas;

20.3. grėsmių ir pažeidimų analizė;

20.4. liekamosios rizikos vertinimas.

21. Rizikos valdymo priemonių planas, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti, tvirtinamas VGI viršininko.

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

22.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

22.2. informacijos saugos priemonės diegimo kainos adekvatumas saugomos informacijos vertei;

22.3. esant galimybei, turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

23. Siekiant užtikrinti Saugos nuostatuose ir Saugos dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, kartą per dvejus metus organizuojamas informacinių technologijų saugos atitikties vertinimas (toliau – Atitikties vertinimas), kurio metu:

23.1. įvertinama esamos informacijos saugos padėties atitiktis Saugos nuostatų ir Saugos dokumentų reikalavimams;

23.2. inventorizuojama VGI IS techninė ir programinė įranga;

23.3. tikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų VGI IS duomenis tvarkančių darbuotojų ir administratorių darbų vietų bei visų tarnybinių stočių programinė įranga ir jų sąranka;

23.4. įvertinama VGI IS duomenis tvarkantiems darbuotojams ir administratoriams suteiktų teisių atitiktis vykdomoms funkcijoms;

23.5. įvertinamas pasirengimas užtikrinti VGI IS veiklos tęstinumą įvykus saugos incidentui.

24. Atlikus Atitikties vertinimą, rengiamas trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato VGI viršininkas.

25. Prireikus Saugos įgaliotinis gali inicijuoti ir VGI viršininko pavedimu atlikti neeilinį VGI IS rizikos įvertinimą.

26. Neeilinis VGI IS rizikos vertinimas turi būti atliekamas:

26.1. įvykus pokyčiams VGI IS techninėje ar programinėje įrangoje, kurie galėtų įtakoti VGI IS veikimą;

26.2. paaiškėjus naujoms tendencijoms informacinių technologijų saugos srityje, dėl kurių kiltų grėsmė VGI IS techninei, programinei įrangai ar VGI IS laikomiems duomenims;

26.3. po saugos incidento, kurio metu būtų sutrikdyta VGI IS veikla, sugadinti ar prarasti VGI IS duomenys.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

27. Priemonės ir metodai, kurie taikomi užtikrinant prieigą prie VGI IS, nurodant leistiną šios prieigos laiką ir būdą, nustatomi VGI IS naudotojų administravimo taisyklėse.

28. Visos VGI IS tarnybinės stotys ir naudotojų darbo vietos turi būti apsaugotos nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.). Apsaugai naudojama programinė įranga turi būti atnaujinama automatiškai ne rečiau kaip kartą per parą.

29. Programinės įrangos naudojimo nuostatos:

29.1. naudojama tik legali ir saugi programinė įranga;

29.2. naudojama tik VGI IS funkcijoms vykdyti būtina programinė įranga;

29.3. programinė įranga atnaujinama laikantis gamintojo reikalavimų;

29.4. rasta nelegali programinė įranga nedelsiant pašalinama;

29.5. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka VGI IS administratorius;

29.6. VGI IS naudotojų kompiuteriuose draudžiama naudoti programinę įrangą, nesusijusią su jų tiesiogine veikla ir funkcijomis.

30. Prieigai prie VGI IS naudojami kompiuteriai gali būti naudojami ir kitoms VGI IS naudotojo ir VGI IS administratoriaus funkcijoms atlikti.

31. VGI IS naudotojų prieiga prie kitų valstybės institucijų, žinybų kompiuterių tinklų ar interneto turi būti apsaugota ugniasienėmis:

31.1. interneto turinys turi būti kontroliuojamas, filtruojant nepageidaujamą informaciją;

31.2. atskiri tinklo segmentai turi būti fiziškai atskirti vienas nuo kito, informacijos apsikeitimas tarp jų turi būti realizuotas ugniasienių pagalba;

31.3. ugniasienių sistema turi būti dubliuota.

32. Naudojami tarnybinės stoties operacinės sistemos metodai, leidžiantys vienareikšmiškai atpažinti kompiuterių tinklui priklausančius kompiuterius.

33. Draudžiama neatpažintiems VGI IS naudotojams prisijungti prie kompiuterių tinklo iš kompiuterio, nepriklausančio šiam tinklui.

34. Draudžiama keisti kompiuterių išdėstymo vietas VGI patalpose be VGI IS administratoriaus leidimo.

35. Kompiuteriai naudojami tik tarnybinėms funkcijoms vykdyti.

36. Tarnybiniai nešiojamieji kompiuteriai ne VGI patalpose gali būti naudojami tik tarnybinėms funkcijoms vykdyti.

37. Iš nutolusių VGI darbo vietų prie VGI IS jungiamasi naudojant virtualų privatų tinklą.

38. Kompiuterius, turinčius prieigą prie VGI IS, naudojant nustatytoms funkcijoms vykdyti ne VGI patalpose, įdiegiamos papildomos saugos priemonės (kietojo disko duomenų šifravimas, rakinimo įrenginių naudojimas).

39. Užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą iš kitų valstybės institucijų, naudojamas Saugus valstybės duomenų perdavimo tinklas (toliau – SVDPT).

40. VGI IS naudotojų kompiuterių tinklai turi 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. įsakyme Nr. 1V-210 „Dėl Saugaus valstybinio duomenų perdavimo tinklo elektroninės informacijos saugos reikalavimų patvirtinimo“ (toliau – Saugaus valstybinio duomenų perdavimo tinklo elektroninės informacijos saugos reikalavimai).

41. SVDPT naudotojų prisijungimui prie SVDPT naudojamas pirmasis prisijungimo būdas, taip kaip tai nurodyta Saugaus valstybinio duomenų perdavimo tinklo elektroninės informacijos saugos reikalavimuose.

42. Duomenys teikiami ir (ar) gaunami automatiniu būdu tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas.

43. Atsarginių kopijų darymas turi užtikrinti VGI IS veiklos tęstinumą:

43.1 tarnybinėse stotyse ir duomenų saugyklose esančios informacijos atsarginės duomenų kopijos daromos automatiškai;

43.2 prarasta, iškraipyta, sunaikinta elektroninė informacija turi būti atkuriama iš informacijos atsarginių kopijų;

43.3. duomenų atkūrimo iš atsarginių kopijų testavimas atliekamas ne rečiau kaip kartą per metus.

44. Prisijungimo prie kompiuterių tinklo laikas ir trukmė nėra ribojami.

45. Kompiuterinė įranga turi rezervinį maitinimo šaltinį (UPS), užtikrinantį šios įrangos veikimą ne mažiau nei 30 min.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

46. Saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo ir valdymo principus (informacijos konfidencialumo, vientisumo, pasiekiamumo, apsaugos) ir priemones (administracines, organizacines, technines), tobulinti kvalifikaciją elektroninės informacijos saugos srityje, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Informacinių technologijų saugos atitikties vertinimo metodika,

patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais.

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

48. VGI IS administratoriumi gali būti skiriamas valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, išmanantis pagrindinius elektroninės informacijos saugos principus, darbą su kompiuterių tinklais ir mokantis užtikrinti jų saugumą. VGI IS administratorius privalo būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais.

49. Visi VGI IS naudotojai privalo turėti darbo kompiuteriu įgūdžių ir mokėti tvarkyti VGI IS duomenis.

50. Tvarkyti VGI IS duomenis gali tik VGI IS naudotojai, susipažinę su VGI IS nuostatais, Saugos nuostatais ir Saugos dokumentais bei raštu sutikę laikytis šių teisės aktų reikalavimų.

51. VGI IS naudotojai, pažeidę Saugos nuostatų ar Saugos dokumentų reikalavimus, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

52. VGI IS naudotojų supažindinimą su Saugos nuostatais, Saugos dokumentais ir kitais saugos politiką įgyvendinančiais teisės aktais ir atsakomybe už reikalavimų, pateiktų šiuose teisės aktuose, nesilaikymą organizuoja Saugos įgaliotinis. Saugos įgaliotinis raštu informuoja VGI IS naudotojus apie Saugos nuostatų, Saugos dokumentų ar kitų saugos politiką įgyvendinančių teisės aktų pripažinimą netekusiais galios, keitimą ar priėmimą.

53. Saugos įgaliotinis organizuoja mokymus ir seminarus duomenų apsaugos klausimais.

54. Saugos įgaliotinis, ne rečiau kaip kartą per dvejus metus esamiems VGI IS naudotojams ir prieš pradedant naudotis VGI IS naujiems VGI IS naudotojams, inicijuoja VGI IS naudotojų mokymą informacijos saugos klausimais. VGI IS naudotojų mokymus informacijos saugos klausimais vykdo VGI IS administratorius arba kitas Saugos įgaliotinio paskirtas asmuo.

55. Mokymai elektroninės informacijos saugos klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į elektroninės informacijos saugumo užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), VGI IS naudotojų ar VGI IS administratoriaus poreikius

56. Mokymų ir seminarų metu VGI IS naudotojai supažindinami su duomenų apsaugos politiką įgyvendinančiais teisės aktais, saugaus darbo su duomenimis principais.

57. VGI sudaro galimybes VGI IS naudotojams dalyvauti Saugos įgaliotinio organizuojamuose kvalifikacijos tobulinimo ir mokymo renginiuose.

V SKYRIUS
VGI IS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

58. Už VGI IS naudotojų supažindinimą su Saugos nuostatais ir Saugos dokumentais bei atsakomybe už šių reikalavimų nesilaikymą yra atsakingas Saugos įgaliotinis.

59. VGI IS tvarkymo įstaigos atsakingi asmenys turi įgyvendinti Saugos nuostatuose ir kituose teisės aktuose, reglamentuojančiuose saugų VGI IS duomenų tvarkymą, nustatytas organizacines, technines ir kitas priemones.

60. Saugos įgaliotinis ir VGI IS administratorius raštu įsipareigoja nepažeisti Saugos nuostatų ir kitų teisės aktų, reglamentuojančių VGI IS duomenų saugų tvarkymą, reikalavimų.

61. VGI IS naudotojai su Saugos nuostatais ir Saugos dokumentais bei atsakomybe už šių teisės aktų reikalavimų nesilaikymą supažindinami pasirašytinai.

62. Saugos įgaliotinis tvarko VGI IS naudotojų supažindinimo su Saugos politika žurnalą, kuriame pildomos šios grafos: supažindinimo data, VGI IS naudotojo vardas ir pavardė, pareigos, parašas.

63. Pakartotinai su Saugos nuostatais ir Saugos dokumentais VGI IS naudotojai supažindinami tik iš esmės pasikeitus VGI IS arba informacijos saugą reglamentuojantiems teisės aktams.

64. Saugos nuostatai ir Saugos dokumentai skelbiami vidiniame VGI tinklalapyje.

65. Saugos įgaliotinis informuoja VGI IS naudotojus elektroniniu paštu ar kitu būdu apie Saugos nuostatų pakeitimus ar kitų saugos politikos įgyvendinamųjų teisės aktų pakeitimus ar minėtų teisės aktų pripažinimą netekusiais galios.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

66. Saugos nuostatai ir Saugos dokumentai turi būti peržiūrėti ne rečiau kaip kartą per kalendorinius metus, atlikus rizikos analizę ar informacinių technologijų saugos atitikties vertinimą, įvykus esminiams organizaciniams, technologiniams ar kitiems VGI IS pokyčiams.

Priedo pakeitimai:
Nr. VE-66, 2016-05-11, paskelbta TAR 2016-05-12, i. k. 2016-12505

Pakeitimai:

1.
Valstybinė geležinkelio inspekcija prie Susisiekimo ministerijos, Įsakymas
Nr. V-419, 2012-07-02, Žin., 2012, Nr. 79-4137 (2012-07-05), i. k. 1122214ISAK000V-419
Dėl Valstybinės geležinkelio inspekcijos prie Susisiekimo ministerijos viršininko 2011 m. vasario 19 d. įsakymo Nr. V-73 "Dėl Geležinkelių transporto valstybinės priežiūros informacinės sistemos duomenų saugos nuostatų patvirtinimo" pakeitimo

2.
Valstybinė geležinkelio inspekcija prie Susisiekimo ministerijos, Įsakymas
Nr. VE-66, 2016-05-11, paskelbta TAR 2016-05-12, i. k. 2016-12505
Dėl Valstybinės geležinkelio inspekcijos prie susisiekimo ministerijos viršininko 2011 m. vasario 19 d. įsakymo Nr. V-73 „Dėl Geležinkelių transporto valstybinės priežiūros informacinės sistemos duomenų saugos nuostatų patvirtinimo“ pakeitimo