PATVIRTINTA
Lietuvos Respublikos susisiekimo ministro
2013 m. gruodžio 27 d.
įsakymu Nr. 3-653

TRANSPORTO PRIEMONIŲ, LAUKIANČIŲ KIRSTI LIETUVOS RESPUBLIKOS VALSTYBĖS SIENĄ, EILIŲ VALDYMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos (toliau – EVIS) saugos politiką, kurios tikslas – nustatyti ir įgyvendinti organizacines, technines ir kitas priemones, suteikiančias galimybę saugiai tvarkyti EVIS duomenis ir užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo ar neteisėto jos tvarkymo.

2. Saugos nuostatuose vartojamos sąvokos suprantamos taip, kaip jos yra apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme (Žin., 2011, Nr. 163-7739), Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarime 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“ (Žin., 2013, Nr. 86-4310), Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 (Žin., 2013, Nr. 23-1122), kituose teisės aktuose ir Lietuvos Respublikos standartuose LST ISO/IEC 27002:2009 ir LST ISO/IEC 27001:2006.

3. Saugos politiką nustato šie susisiekimo ministro patvirtinti teisės aktai (toliau – saugos politikos įgyvendinamieji dokumentai):

3.1. Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės;

3.2. Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos naudotojų administravimo taisyklės;

3.3. Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos veiklos tęstinumo valdymo planas.

Saugos nuostatai kartu su saugos politikos įgyvendinamaisiais dokumentais sudaro saugos dokumentus.

4. EVIS duomenų saugos tikslas – užtikrinti EVIS duomenų patikimumą, konfidencialumą, prieinamumą, vientisumą ir tinkamą kompiuterinės, programinės ir ryšių įrangos funkcionavimą.

5. EVIS duomenų saugos užtikrinimo prioritetinės kryptys:

5.1. EVIS duomenims tvarkyti naudojamos techninės ir programinės įrangos kontrolė;

5.2. EVIS duomenų tvarkymo kontrolė;

5.3. saugaus darbo su EVIS duomenimis kontrolė;

5.4. fizinė EVIS duomenų tvarkymo priemonių (tarnybinių stočių, informacijos perdavimo įrangos, programinės įrangos) ir patalpų apsauga.

6. Saugos nuostatais privalo vadovautis EVIS saugos įgaliotinis (toliau – saugos įgaliotinis), EVIS administratorius (-iai) (toliau – administratorius), EVIS duomenų valdymo įgaliotinis, EVIS naudotojai ir kiti subjektai, kuriems taikomi Saugos nuostatų reikalavimai.

7. EVIS valdytoja yra Lietuvos Respublikos susisiekimo ministerija (Gedimino pr. 17, 01505 Vilnius), EVIS tvarkytoja yra Pasienio kontrolės punktų direkcija prie Susisiekimo ministerijos (Gedimino pr. 26, 01104 Vilnius).

8. EVIS valdytojo funkcijos ir atsakomybė:

8.1. atsako už EVIS saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą;

8.2. tvirtina EVIS saugos dokumentus ir kontroliuoja, kad EVIS būtų tvarkoma vadovaujantis šiais dokumentais;

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

8.4. atsako už EVIS pokyčių ir plėtros įgyvendinimą;

8.5. pagal kompetenciją atsako už EVIS duomenų saugą;

8.6. paveda EVIS tvarkytojui paskirti saugos įgaliotinį, duomenų valdymo įgaliotinį, administratorių;

8.7. sudaro sutartis su duomenų gavėjais.

9. EVIS tvarkytojo funkcijos ir atsakomybė:

9.1. atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatų ir saugos politikos įgyvendinamųjų dokumentų nustatyta tvarka;

9.2. EVIS tvarkytojo vadovas įsakymu paskiria saugos įgaliotinį, duomenų valdymo įgaliotinį ir administratorių;

9.3. rengia EVIS saugos dokumentus ir teikia juos tvirtinti EVIS valdytojo vadovui;

9.4. teikia EVIS valdytojui pasiūlymus dėl EVIS plėtros, saugos ir funkcionalumo;

9.5. organizuoja plėtrą ir EVIS pakeitimų įdiegimą;

9.6. rūpinasi EVIS duomenų saugumu ir užtikrina tinkamą EVIS administravimą;

9.7. užtikrina EVIS saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams ir Saugos nuostatams;

9.8. atlieka kitas EVIS valdytojo pavestas ir teisės aktuose priskirtas funkcijas.

10. Saugos įgaliotinio funkcijos ir atsakomybė:

10.1. teikia siūlymus EVIS tvarkytojo vadovui dėl:

10.1.1 administratoriaus paskyrimo ir reikalavimų administratoriui nustatymo;

10.1.2. informacinių technologijų saugos atitikties vertinimo atlikimo;

10.1.3. saugos dokumentų priėmimo ir keitimo;

10.2. atsako už tinkamą EVIS saugos reikalavimų ir funkcijų vykdymą;

10.3. organizuoja rizikos įvertinimą, prireikus – neeilinį EVIS rizikos įvertinimą ir EVIS informacinių technologijų saugos atitikties vertinimą;

10.4. teikia administratoriui ir EVIS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;

10.5. koordinuoja saugos dokumentų nuostatų pažeidimų ir (ar) saugos incidentų tyrimus;

10.6. bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais;

10.7. užtikrina EVIS saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams;

10.8. pasirašytinai supažindina administratorius ir EVIS naudotojus su saugos dokumentais ir atsakomybe už šių dokumentų reikalavimų nesilaikymą;

10.9. periodiškai inicijuoja administratoriaus ir EVIS naudotojų mokymus informacijos saugos klausimais (teminių seminarų rengimas, atmintinės naujai priimtiems darbuotojams ir pan.);

10.10. atlieka kitas EVIS tvarkytojo vadovo pavestas užduotis ir teisės aktuose priskirtas funkcijas.

11. Saugos įgaliotinis negali atlikti administratoriaus funkcijų.

12. Administratoriaus funkcijos ir atsakomybė:

12.1. atlieka EVIS naudotojams priskirtų funkcijų ir suteiktų teisių atitikties vertinimą, administruoja šias teises;

12.2. rengia ir tikrina EVIS sudarančių komponentų sąranką;

12.3. vykdo EVIS sudarančių dalių (kompiuterių, operacinės sistemos, duomenų bazių valdymo sistemos, taikomųjų programų sistemos, ugniasienės, įsilaužimo aptikimo sistemos, duomenų perdavimo tinklų ir kt.) priežiūrą, kontroliuoja ir atsako už EVIS ir ją sudarančių komponentų nepertraukiamą veikimą;

12.4. registruoja elektroninės informacijos saugos incidentus ir informuoja saugos įgaliotinį apie nustatytus saugos politikos pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones;

12.5. nustato EVIS pažeidžiamas vietas ir informuoja apie jas saugos įgaliotinį;

12.6. užtikrina, kad būtų laikomasi saugos dokumentų ir kitų teisės aktų reikalavimų;

12.7. vykdo saugos įgaliotinio nurodymus ir pavedimus, susijusius su EVIS duomenų saugos užtikrinimu;

12.8. įregistruoja ir išregistruoja EVIS naudotojus;

12.9. įdiegia programinės įrangos atnaujinimus, nustato automatinio atnaujinimo procedūras;

12.10. tikrina pranešimus apie serverių operacinių sistemų ir duomenų bazių valdymo sistemų klaidas ir imasi būtinų priemonių, kad būtų išvengta galimų gedimų;

12.11. jeigu administruojamas nutolęs serveris ir nustatomas sutrikimas, kurio negalima pašalinti nuotolinėmis priemonėmis, susisiekia su asmenimis, įgaliotais atlikti techninę priežiūrą nutolusioje vietovėje, ir prižiūri sutrikimų šalinimo eigą;

12.12. užtikrina visų prisijungimo vardų, slaptažodžių apsaugą;

12.13. teikia siūlymus EVIS tvarkytojo vadovui dėl EVIS kūrimo, funkcionalumo užtikrinimo, priežiūros ir duomenų saugos klausimų;

12.14. daro atsargines EVIS duomenų kopijas;

12.15. atlieka kitas EVIS tvarkytojo vadovo pavestas užduotis ir teisės aktuose priskirtas funkcijas.

13. Teisės aktų, kuriais vadovaujamasi tvarkant EVIS duomenis ir užtikrinant jų saugumą, sąrašas:

13.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

13.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (Žin., 1996, Nr. 63-1479; 2008, Nr. 22-804);

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

13.4. 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 (Žin., 2013, Nr. 106-5251);

13.5. Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtinti Valstybės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. IT-71(1.12) (Žin., 2008, Nr. 135-5298);

13.6. Lietuvos standartai LST ISO/IEC 27002:2009 ir LST ISO/IEC 27001:2006, Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo technika" grupės standartai, nustatantys saugų informacinės sistemos duomenų tvarkymą;

13.7. Saugos nuostatai;

13.8. saugos politikos įgyvendinamieji dokumentai;

13.9. kiti teisės aktai.

II. EVIS DUOMENŲ SAUGOS VALDYMAS

14. Pagal Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 (Žin., 2013, Nr. 86-4310), 4.3.1 ir 4.3.2 punktus EVIS tvarkoma elektroninė informacija priskirtina žinybinės svarbos elektroninės informacijos kategorijai.

15. Pagal Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 5.3 punktą EVIS priskiriama trečios kategorijos informacinei sistemai, atsižvelgiant į joje apdorojamos elektroninės informacijos svarbą.

16. Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas", Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika" grupės standartus, kasmet organizuoja EVIS rizikos vertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį rizikos vertinimą. EVIS rizikos vertinimas atliekamas pagal kokybinį rizikos vertinimo metodą. EVIS tvarkytojo rašytiniu pavedimu EVIS rizikos įvertinimą gali atlikti pats saugos įgaliotinis.

17. EVIS rizikos įvertinimo rezultatai pateikiami rizikos įvertinimo ataskaitoje, kuri pateikiama EVIS tvarkytojo vadovui. Rizikos įvertinimo ataskaita rengiama įvertinant rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausieji rizikos veiksniai yra šie:

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

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

17.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 (Žin., 1996, Nr. 68-1652), 3 punkte.

18. Rizikos veiksniai vertinami pagal elektroninės informacijos kategorijas, nustatant jų pasireiškimo dažnio ir įtakos EVIS elektroninės informacijos saugai laipsnius:

18.1. Žemas (Ž) – pasireiškia vieną kartą per mėnesį, duomenų pažeidimo poveikio laipsnis nėra didelis, padariniai nebus pavojingi – dingo ar yra sugadinta iki 5 proc. informacijos; atskleista 5 proc. neviešos (pavyzdžiui, asmens duomenys) informacijos; EVIS neprieinama ne daugiau nei 20 min. Visa sugadinta informacija EVIS priemonėmis yra atkuriama iš atsarginių kopijų per 1 valandą.

18.2. Vidutinis (V) – pasireiškia daugiau nei vieną kartą per mėnesį, duomenų pažeidimo poveikio laipsnis gali būti didelis, padariniai rimti – dingo ar yra sugadinta mažiau kaip 50 proc. informacijos; atskleista 20 proc. neviešos (pavyzdžiui, asmens duomenys) informacijos; EVIS neprieinama ne daugiau kaip 35 min. Visa sugadinta informacija EVIS priemonėmis yra atkuriama iš atsarginių kopijų per 1 valandą.

18.3. Aukštas (A) – pasireiškia daugiau nei 3 kartus per mėnesį, duomenų pažeidimo poveikio laipsnis labai didelis, padariniai rimti – dingo ar yra sugadinta daugiau kaip 50 proc. informacijos; atskleista 35 proc. neviešos (pavyzdžiui, asmens duomenys) informacijos; EVIS neprieinama daugiau kaip 50 min. Dalis informacijos (ne mažiai kaip 30 proc.) EVIS priemonėmis yra atkuriama iš atsarginių kopijų per 1 valandą.

19. Rizikos vertinimo metu atliekamos veiklos:

19.1. EVIS sudarančių informacinių išteklių inventorizacija;

19.2. įtakos EVIS veiklai vertinimas;

19.3. grėsmės ir pažeidimų analizė;

19.4. liekamosios rizikos vertinimas.

20. Atsižvelgdamas į rizikos įvertinimo ataskaitą, EVIS valdytojas prireikus tvirtina rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

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

21.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

21.2. informacijos saugos priemonės diegimo kainos atitiktis saugomos informacijos vertei;

21.3. esant galimybei, turi būti įdiegtos prevencinės korekcinės informacijos saugos priemonės.

22. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas EVIS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti per Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemą Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

23. Siekiant užtikrinti Saugos nuostatų ir saugos politikos įgyvendinamųjų dokumentų nuostatų įgyvendinimo kontrolę, ne rečiau kaip kartą per metus organizuojamas informacinių technologijų saugos atitikties vertinimas, vadovaujantis Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 (Žin., 2004, Nr. 80-2855).

24. Atliekant EVIS informacinių technologijų saugos atitikties vertinimą yra:

24.1. įvertinama esamos EVIS duomenų saugos situacijos atitiktis EVIS saugos dokumentams ir kitiems duomenų saugą reglamentuojantiems teisės aktams;

24.2. inventorizuojama EVIS techninė ir programinė įranga;

24.3. peržiūrima administratoriui ir EVIS naudotojams suteiktų teisių atitiktis jų atliekamoms funkcijoms;

24.4. duomenų saugos požiūriu patikrinama EVIS techninė ir programinė įranga: visos tarnybinės stotys ir ne mažiau kaip 10 procentų atsitiktinai parinktų EVIS naudotojų darbo vietų;

24.5. įvertinamas pasirengimas užtikrinti EVIS veiklos tęstinumą įvykus elektroninės informacijos saugos incidentui.

25. Atlikus EVIS informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama EVIS tvarkytojo vadovui, ir pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato EVIS valdytojo vadovas.

26. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas EVIS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti per Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemą Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

27. Prireikus saugos įgaliotinis gali organizuoti neeilinį EVIS informacinių technologijų saugos atitikties vertinimą.

28. Neeilinis EVIS informacinių technologijų saugos atitikties vertinimas atliekamas:

28.1. įvykus EVIS techninės ar programinės įrangos pokyčiams, kurie gali turėti įtakos EVIS veikimui;

28.2. paaiškėjus naujoms tendencijoms informacinių technologijų saugos srityje, dėl kurių kiltų grėsmė EVIS techninei, programinei įrangai ar EVIS tvarkomiems duomenims;

28.3. po saugos incidento, kurio metu sutrikdyta EVIS veikla, sugadinti ar prarasti EVIS duomenys.

III. EVIS ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

29. Metodai ir priemonės, kurie taikomi užtikrinant prieigą prie EVIS:

29.1. EVIS naudotojai privalo turėti galimybę naudotis tik tokiomis teisėmis ir tais duomenimis, kurie jiems numatyti nustačius prieigos prie EVIS teises, įgyvendinant principą „būtina žinoti“;

29.2. EVIS priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą administratoriaus klasifikatorių, kuriuo naudojantis nebūtų galima atlikti EVIS naudotojo funkcijų;

29.3. kiekvienas EVIS naudotojas turi būti EVIS unikaliai identifikuojamas – EVIS naudotojas turi patvirtinti savo tapatybę slaptažodžiu arba kita autentiškumo patvirtinimo priemone;

29.4. EVIS turi registruoti paskutinį EVIS elektroninės informacijos pakeitimą atlikusį EVIS naudotoją ir pakeitimo laiką;

29.5. patalpose, kuriose yra EVIS duomenų centras, turi būti įrengti ir prie pastato signalizacijos ir apsaugos tarnybų prijungti gaisro ir įsilaužimo davikliai;

29.6. duomenų centro patalpose turi būti įrengta stebėjimo sistema su įrašymo funkcija.

30. Programinės įrangos, skirtos EVIS apsaugoti nuo kenksmingos programinės įrangos, naudojimo nuostatos:

30.1. EVIS turi būti naudojama antivirusinė programinė įranga, skirta EVIS apsaugoti nuo kenksmingos programinės įrangos;

30.2. antivirusinė programinė įranga turi būti atnaujinama automatiškai ne rečiau kaip kartą per parą;

30.3. turi būti operatyviai ne vėliau kaip per 5 (penkias) darbo dienas įdiegiamos EVIS operacinės sistemos ir naudojami programinės įrangos gamintojų rekomenduojami atnaujinimai;

30.4. EVIS turi būti naudojama tik licencijuota programinė įranga.

31. Programinės įrangos naudojimo nuostatos:

31.1. EVIS tarnybinėse stotyse negali būti įdiegta programinės įrangos, kuri yra nesusijusi su EVIS veikla;

31.2. naudotojai naudojasi prieiga prie EVIS per išorinį portalą; prisijungimo laikas nėra ribojamas;

31.3. EVIS naudotojams, kuriems atliekant tiesiogines pareigas būtina prisijungti iš nutolusios darbo vietos, gali būti suteikiama nuotolinio prisijungimo prie EVIS galimybė;

31.4. techninis nuotolinio prisijungimo sprendimas turi užtikrinti ne žemesnį nei vidiniam prisijungimui naudojamą saugumo lygį, t. y. turi būti naudojamos Saugos nuostatuose minimos priemonės ir duomenų šifravimas naudojantis virtualiu privačiu tinklu (angl. *virtual private network* – VPN);

31.5. prie EVIS prisijungiama nuotoliniu būdu naudojant interneto naršyklę (https protokolą);

31.6. kompiuterinis tinklas, prie kurio prijungtos EVIS tarnybinės stotys ir EVIS naudotojų kompiuteriai, nuo viešojo interneto turi būti atskirtas tinklo užkarda, už kurios administravimą ir priežiūrą atsakingas administratorius;

31.7. EVIS naudotojui teisė dirbti su konkrečia elektronine informacija turi būti ribojama ar sustabdoma, kai EVIS naudotojas atostogauja, vykdomas EVIS naudotojo veiklos tyrimas ir pan.; pasibaigus tarnybos (darbo) santykiams, EVIS naudotojo teisė naudotis EVIS turi būti panaikinta;

31.8. baigus darbą, turi būti imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys, – atsijungiama nuo EVIS, įjungiama ekrano užsklanda su slaptažodžiu, dokumentai padedami į pašaliniams asmenims neprieinamą vietą;

31.9. EVIS naudotojui neatliekant jokių veiksmų, EVIS turi užsirakinti, kad toliau naudotis EVIS galima būtų tik pakartojus tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus.

32. Kompiuterių (įskaitant nešiojamuosius) naudojimo reikalavimai:

32.1. stacionarūs ir nešiojamieji EVIS naudotojų kompiuteriai turi būti naudojami tik su tiesioginių pareigų atlikimu susijusiai veiklai; iš kompiuterių, kurie perduodami remontui ar techninei priežiūrai, turi būti pašalinta visa riboto naudojimo EVIS elektroninė informacija;

32.2. visiems EVIS naudotojų kompiuteriams turi būti naudojamos papildomos saugos priemonės, kuriomis patvirtinama kompiuterio naudotojo tapatybė.

33. Metodai, kuriais gali būti užtikrinamas saugus EVIS duomenų teikimas ir (ar) gavimas:

33.1. EVIS duomenys perduodami automatiniu būdu (naudojant TCP/IP protokolą) realiu laiku arba asinchroniniu režimu pagal EVIS duomenų teikimo ir gavimo sutartis, kuriose nustatytos perduodamų duomenų specifikacijos, perdavimo sąlygos ir tvarka;

33.2. už duomenų teikimo ir gavimo sutartyse nurodomų saugos reikalavimų nustatymą, suformulavimą ir įgyvendinimo organizavimą atsakingas saugos įgaliotinis.

34. Pagrindiniai atsarginių EVIS duomenų kopijų darymo ir atkūrimo reikalavimai:

34.1. privalo būti visų saugomų duomenų rezervinio kopijavimo funkcija;

34.2. privalo būti galimybė daryti rezervines kopijas ir veikiant, ir neveikiant programinei įrangai;

34.3. administratorius privalo turėti galimybę inicijuoti duomenų atkūrimo iš rezervinės kopijos procedūrą pasirinktinai iš turimų rezervinių kopijų sąrašo; atkūrus duomenis privalo būti užtikrintas ir išlaikytas duomenų vientisumas ir integralumas;

34.4. EVIS duomenys EVIS naudotojams turi būti prieinami ne mažiau kaip 99,30 proc. laiko per mėnesį;

34.5. jeigu neveikia EVIS ar jos dalis ir dėl to nutrūksta transporto priemonių eilių elektroninis reguliavimas, ne vėliau kaip per dvi valandas turi būti atkurtas EVIS funkcionalumas; poste priešais pasienio kontrolės punktą EVIS naudotojams turi būti sudaryta galimybė nuolat gauti duomenis apie registruotas transporto priemones iš atsarginio informacijos šaltinio, kuriame

reguliariai išsaugomi duomenys apie registruotas transporto priemones; vadovaudamiesi šiais duomenimis, EVIS naudotojai leis įvažiuoti transporto priemonėms į pasienio kontrolės punktą, kol bus atkurtas EVIS funkcionalumas;

34.6. ne rečiau kaip vieną kartą per mėnesį administratorius pateikia EVIS valdytojui programinės įrangos ir duomenų kopijas skaitmeninėje laikmenoje, kurios turi leisti atkurti informacinę sistemą įvykus gedimui; EVIS duomenų atsarginės kopijos yra daromos ir saugomos taip, kad jos nebūtų prieinamos tretiesiems asmenims, kurie neturi teisės su jomis dirbti; EVIS atsarginės elektroninės informacijos kopijos turi būti laikomos atskiroje (nuo pagrindinių duomenų) patalpoje ir saugomos užrakintoje nedegioje spintoje; už atsarginių kopijų darymą ir atkūrimą atsakingas administratorius; atkūrimo iš atsarginių kopijų funkcija privalo būti išbandoma ne rečiau kaip kartą per metus; duomenų atkūrimo bandymą organizuoja saugos įgaliotinis.

IV. REIKALAVIMAI PERSONALUI

35. Saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus ir metodus, rizikų valdymą, tobulinti kvalifikaciją elektroninės informacijos saugos srityje ir savo darbe vadovautis saugos dokumentais, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 (Žin., 2013, Nr. 86-4310), Informacinių technologijų saugos atitikties vertinimo metodika ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugos klausimus.

36. Administratorius privalo išmanyti darbą su kompiuterių tinklais ir mokėti užtikrinti jų saugumą, būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais.

37. Visi EVIS naudotojai privalo turėti darbo kompiuteriu įgūdžių.

38. Tvarkyti EVIS duomenis EVIS naudotojai gali tik susipažinę su EVIS nuostatais, Saugos nuostatais ir saugos politikos įgyvendinamaisiais dokumentais ir raštu sutikę laikytis šių teisės aktų reikalavimų.

39. EVIS naudotojai privalo rūpintis tvarkomų duomenų saugumu. Įpareigojimas saugoti tvarkomų duomenų paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą.

40. EVIS naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias EVIS saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti EVIS administratoriui ir saugos įgaliotiniui, o jo nesant – EVIS administratoriui. Jeigu saugos įgaliotinis nebuvo informuotas apie šiame punkte nurodytus pažeidimus, administratorius informuoja saugos įgaliotinį apie šiuos pažeidimus.

41. EVIS naudotojų mokymai organizuojami taip, kaip numatyta Saugos nuostatų 10.9 punkte, ne rečiau kaip kartą per metus.

V. EVIS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

42. EVIS tvarkytojo vadovas užtikrina, kad EVIS naudotojai būtų supažindinti su EVIS saugos dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą ir atsakomybę už šių teisės nuostatų pažeidimus.

43. Už EVIS naudotojų supažindinimą su EVIS saugos dokumentais ir atsakomybe, kylančia dėl jų pažeidimo, atsakingas saugos įgaliotinis.

44. EVIS naudotojus su saugos dokumentais ir teisės aktais, reglamentuojančiais EVIS duomenų saugą, saugos įgaliotinis pasirašytinai supažindina prieš sukurdamas EVIS naudotojo prisijungimo duomenis.

45. Pakartotinai su saugos dokumentais ir teisės aktais, reglamentuojančiais EVIS duomenų saugą, saugos įgaliotinis pasirašytinai supažindina EVIS naudotojus kitą darbo dieną po saugos dokumentų ir teisės aktų, reglamentuojančių EVIS duomenų saugą, priėmimo (išdėstymo nauja redakcija), pakeitimo ar pripažinimo netekusiais galios.

VI. BAIGIAMOSIOS NUOSTATOS

46. Saugos įgaliotinis organizuoja saugos dokumentų peržiūrą ne rečiau kaip kartą per metus. Saugos dokumentai turi būti peržiūrimi atlikus rizikos analizę ar informacinių technologijų saugos atitikties vertinimą, pasikeitus saugos politiką reglamentuojantiems teisės aktams, įvykus esminiams organizaciniams, technologiniams ar kitiems EVIS pokyčiams.

47. Saugos įgaliotinis, administratorius (-iai), EVIS naudotojai ir kiti subjektai, kuriems taikomi Saugos nuostatų reikalavimai, pažeidę saugos politikos įgyvendinamųjų dokumentų reikalavimus, atsako teisės aktų nustatyta tvarka.

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2013 m. gruodžio 13 d. raštu Nr. 1D-11136(52)