Suvestinė redakcija nuo 2009-11-13 iki 2012-02-22

Įsakymas paskelbtas: Žin. 2005, Nr. 150-5512, i. k. 1052210ISAK0003-568

Nauja redakcija nuo 2009-11-13:
Nr. 3-547, 2009-11-03, Žin. 2009, Nr. 135-5899 (2009-11-12), i. k. 1092210ISAK0003-547

LIETUVOS RESPUBLIKOS SUSISIEKIMO MINISTRAS

ĮSAKYMAS DĖL LIETUVOS RESPUBLIKOS JŪRŲ LAIVŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2005 m. gruodžio 15 d. Nr. 3-568
Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės registrų įstatymo (Žin., 1996, Nr. 86-2043; 2004, Nr. 124-4488) 20 straipsnio 3 dalimi, Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų, patvirtintų Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891), 6 punktu bei Saugos dokumentų turinio gairių, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070), nuostatomis ir Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniais saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2008 m. spalio 27 d. įsakymu Nr. 1V-384 (Žin., 2008, Nr. 127-4866):

1. T v i r t i n u Lietuvos Respublikos jūrų laivų registro duomenų saugos nuostatus (pridedama).

2. S k i r i u Lietuvos saugios laivybos administracijos Informacinių technologijų skyriaus vyriausiąją specialistę Neringą Kuzminskienę Lietuvos Respublikos jūrų laivų registro duomenų saugos įgaliotine.

3. P a v e d u Lietuvos saugios laivybos administracijai ne vėliau kaip per 6 mėnesius nuo šio įsakymo įsigaliojimo dienos teisės aktų nustatyta tvarka parengti ir pateikti Lietuvos Respublikos susisiekimo ministrui tvirtinti Lietuvos Respublikos jūrų laivų registro saugaus elektroninės informacijos tvarkymo taisykles, Lietuvos Respublikos jūrų laivų registro veiklos tęstinumo valdymo planą ir Lietuvos Respublikos jūrų laivų registro naudotojų administravimo taisykles.

SUSISIEKIMO MINISTRAS PETRAS ČĖSNA

PATVIRTINTA
Lietuvos Respublikos susisiekimo
ministro 2005 m. gruodžio 15 d.
įsakymu Nr. 3-568
(Lietuvos Respublikos susisiekimo
ministro 2009 m. lapkričio 3 d.
įsakymo Nr. 3-547 redakcija)

LIETUVOS RESPUBLIKOS JŪRŲ LAIVŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos jūrų laivų registro duomenų saugos nuostatų (toliau – Saugos nuostatai) tikslas – sudaryti sąlygas saugiai automatizuotu būdu tvarkyti Lietuvos Respublikos jūrų laivų registro (toliau – Registras) duomenis.

2. Saugos nuostatai reglamentuoja elektroninės informacijos saugos valdymą, organizacinius ir techninius reikalavimus, reikalavimus personalui, dirbančiam su Registru, Registro naudotojų supažindinimo su saugos dokumentais principus.

3. Saugos nuostatai parengti vadovaujantis Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, patvirtintais Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891), Saugos dokumentų turinio gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070), ir Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniais saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2008 m. spalio 27 d. įsakymu Nr. 1V-384 (Žin., 2008, Nr. 127-4866).

4. Registro duomenų saugos tikslas – užtikrinti registro duomenų elektroninės informacijos konfidencialumą, prieinamumą, vientisumą ir tinkamą kompiuterizuotų darbo vietų bei tinklo įrangos funkcionavimą. Registro duomenų saugumui užtikrinti kompleksiškai naudojamos administracinės, techninės ir programinės priemonės, padedančios įgyvendinti reagavimo, atsakomybės, elektroninės informacijos saugos suvokimo kėlimo ir saugos priemonių projektavimo ir diegimo principus.

5. Pagrindinės šiuose Saugos nuostatuose vartojamos sąvokos:

Saugos politika – pagrindinės taisyklės, pagrindiniai taikytini informacijos saugos užtikrinimo ir valdymo principai, į kuriuos atsižvelgiant turi būti derinami informacinės sistemos veiklos ir naudojimo procesai, procedūros ir rengiami juos reglamentuojantys dokumentai;

Registro administratorius – Registro tvarkymo įstaigos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, atliekantis informacinių technologijų taikomųjų sistemų, duomenų bazių, tarnybinių stočių, tinklo ir kitos kompiuterinės įrangos priežiūrą;

Elektroninė informacija – visa informacija, kuri tvarkoma Registro priemonėmis. Tai programos, elektroninės bylos ir kita informacija, kuri saugoma, perduodama ir sukuriama kompiuteriu;

Elektroninės informacijos saugos incidentas – įvykis ar veiksmas, kuris gali sudaryti neteisėto prisijungimo prie Registro galimybę, sutrikdyti ar pakeisti Registro veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti;

Informacijos tvarkymas – visos su informacija atliekamos operacijos: rinkimas, užrašymas, klasifikavimas, grupavimas, kaupimas, saugojimas, keitimas, kopijavimas, sujungimas, atskleidimas, teikimas, naudojimas, naikinimas;

Kompiuterinė įranga – kompiuteriai, tarnybinės stotys, jų dalys, išoriniai įrenginiai

(monitoriai, skeneriai, spausdintuvai bei kopijavimo aparatai, klaviatūros, pelės, garso kolonėlės, ausinės, filmavimo kameros, fotoaparatai, projektoriai ir pan.), kompiuterinio tinklo įranga, kompiuterinės bei tinklinės įrangos montavimo spintos, nepertraukiamo elektros maitinimo šaltiniai ir pan.;

Kompiuterių tinklas – tarnybinė stotis ir darbo vietų kompiuteriai, kompiuterine įranga (kabeliais ir kompiuterių tinklo aparatūra) sujungti į sistemą, siekiant užtikrinti vartotojams operatyvų pasikeitimą informacija, kolektyvinį kompiuterinės ir programinės įrangos naudojimą bei interneto paslaugas;

Programinė įranga – programos, skirtos kompiuterinei įrangai valdyti bei vartotojo uždaviniams spręsti kompiuteriu (operacinės sistemos, programavimo sistemos, biuro programų paketai, antivirusinės, archyvavimo bei kitos taikomosios programos);

Registro naudotojas – Registro tvarkymo įstaigos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, taip pat kitas asmuo, turintis teisę naudotis Registro duomenimis numatytoms funkcijoms atlikti;

Saugos įgaliotinis – Registro tvarkymo įstaigos valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį, įgyvendinantis elektroninės informacijos saugą Registre.

Kitos Saugos nuostatuose vartojamos sąvokos atitinka sąvokas, nustatytas Lietuvos Respublikos įstatymuose ir kituose teisės aktuose bei Lietuvos ir tarptautiniuose „Informacijos technologija. Saugumo metodai“ grupės standartuose, apibūdinančiuose saugų informacinės sistemos duomenų tvarkymą.

6. Saugos nuostatai privalomi visiems Registro naudotojams, saugos įgaliotiniui ir Registro administratoriui.

7. Saugos politiką apibrėžia Saugos nuostatai. Saugos nuostatus įgyvendina Lietuvos Respublikos jūrų laivų registro saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Tvarkymo taisyklės), Lietuvos Respublikos jūrų laivų registro veiklos tęstinumo valdymo planas (toliau – Valdymo planas), Lietuvos Respublikos jūrų laivų registro naudotojų administravimo taisyklės (toliau – Administravimo taisyklės), kiti teisės aktai, reglamentuojantys Registro duomenų tvarkymo teisėtumą ir saugos valdymą.

8. Pagrindinės Registro duomenų saugumo užtikrinimo kryptys:

8.1. atliekamų veiksmų su Registro duomenimis automatinio stebėjimo ir įrašų kaupimo įgyvendinimas;

8.2. prieigos teisių prie Registro duomenų suteikimo ir duomenų vartotojo tapatumo identifikavimo įgyvendinimas;

8.3. Registro duomenų kopijavimo, archyve esančių duomenų saugos įgyvendinimas;

8.4. Registro duomenų saugos nuo žalingos programinės įrangos poveikio įgyvendinimas;

8.5. saugių Registrui tvarkyti skirtų patalpų ir kompiuterizuotų darbo vietų jose įrengimas;

8.6. Registro naudotojų kvalifikacijos tobulinimo sistemos įgyvendinimas;

8.7. Registro duomenų integralumo su kitais registrais ir informacinėmis sistemomis užtikrinimas;

8.8. Registro duomenų saugos priemonių nuo nesankcionuoto poveikio Registro programinei, techninei įrangai ir (ar) Registro programinės įrangos modifikavimo įgyvendinimas.

9. Vadovaujančioji Registro tvarkymo įstaiga yra Lietuvos Respublikos susisiekimo ministerija (toliau – Susisiekimo ministerija), Gedimino pr. 17, LT-01505 Vilnius. Susisiekimo ministerija yra ir Registre tvarkomų asmens duomenų valdytoja.

Registro tvarkymo įstaiga – Lietuvos saugios laivybos administracija (toliau – Administracija), J. Janonio g. 24, LT-92251 Klaipėda, Registro duomenis tvarko pagal Lietuvos Respublikos jūrų laivų registro nuostatų, patvirtintų Lietuvos Respublikos Vyriausybės 2004 m. spalio 21 d. nutarimu Nr. 1318 (Žin., 2004, Nr. 156-5703), reikalavimus. Administracija yra Registre tvarkomų asmens duomenų tvarkytoja. Ji taip pat vykdo Registro duomenų bazės tvarkytojos funkcijas.

10. Susisiekimo ministro funkcijos ir atsakomybė:

10.1. vadovauja ir organizuoja Registro veiklą;

10.2. tvirtina saugos dokumentus;

10.3. prižiūri saugos dokumentų įgyvendinimą;

10.4. skiria saugos įgaliotinį;

10.5. kontroliuoja, kad Registras būtų tvarkomas vadovaujantis Lietuvos Respublikos įstatymais ir kitais teisės aktais.

11. Administracijos direktoriaus funkcijos ir atsakomybė:

11.1. rūpinasi Registro duomenų sauga;

11.2. atsako už Registro saugos reikalavimų atitiktį Saugos nuostatams ir kitiems galiojantiems Lietuvos Respublikos teisės aktams;

11.3. paveda saugos įgaliotiniui organizuoti ir kontroliuoti saugos politiką reglamentuojančių teisės aktų įgyvendinimą Administracijoje;

11.4. paskiria Registro administratorių, jam paveda užtikrinti Registro tarnybinės stoties saugų funkcionavimą ir Registro naudotojų kompiuterinių darbo vietų programinės įrangos priežiūrą, kontrolę ir tinkamo veikimo užtikrinimą, administruoja Registro duomenų bazę Saugos nuostatų ir kitų saugos politiką reglamentuojančių teisės aktų nustatyta tvarka;

11.5. nustato reikalavimus saugos įgaliotinio, Registro administratoriaus ir Registro naudotojų kvalifikacijai.

12. Saugos įgaliotinio, įgyvendinančio Registro elektroninės informacijos saugą, funkcijos ir atsakomybė:

12.1. teikia Administracijos direktoriui pasiūlymus dėl:

12.1.1. Registro administratoriaus paskyrimo;

12.1.2. saugos dokumentų priėmimo, keitimo ar panaikinimo;

12.1.3. Registro informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

12.2. koordinuoja elektroninės informacijos saugos incidentų tyrimą;

12.3. pasirašytinai supažindina Registro administratorių, Registro naudotojus su Saugos nuostatais ir saugos politiką įgyvendinančiais teisės aktais bei atsakomybe už šių reikalavimų nesilaikymą;

12.4. organizuoja Registro administratoriaus ir Registro naudotojų kvalifikacijos tobulinimą duomenų saugos klausimais, reguliariai jiems primena Registro saugos problemas (elektroniniu paštu, atmintinės naujai priimtiems darbuotojams ir pan.);

12.5. atsako už Registro saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams;

12.6. teikia Registro administratoriui privalomus vykdyti nurodymus ir pavedimus;

12.7. atlieka kitas Administracijos direktoriaus pavestas ir priskirtas funkcijas.

13. Registro administratoriaus funkcijos ir atsakomybė:

13.1. atsako už Registro funkcionavimą;

13.2. įvertina Registro naudotojų pasirengimą dirbti su Registru ir suteikia Registro naudotojams teisę naudotis Registro galimybėmis paskirtoms funkcijoms atlikti;

13.3. rengia pasiūlymus Registro kūrimo, palaikymo, priežiūros ir duomenų saugos klausimais;

13.4. atlieka Registro sudarančių komponentų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, įsilaužimų aptikimo sistemų, duomenų perdavimo tinklų) administravimą, pažeidžiamų vietų ir saugos reikalavimų atitikties nustatymą;

13.5. registruoja elektroninės informacijos saugos incidentus, apie juos informuoja saugos įgaliotinį ir teikia dėl jų pasiūlymus;

13.6. užtikrina Registro naudotojų kompiuterinių darbo vietų programinės įrangos priežiūrą, kontrolę ir tinkamą veikimą.

14. Registro duomenų sauga užtikrinama vadovaujantis Lietuvos Respublikos valstybės registrų įstatymu (Žin., 1996, Nr. 86-2043; 2004, Nr. 124-4488), Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, Saugos dokumentų turinio gairėmis, Lietuvos standartu LST ISO/IEC 17799:2005, Lietuvos ir tarptautiniais

„Informacijos technologija. Saugumo technika“ grupės standartais, Saugos nuostatais, Tvarkymo taisyklėmis, Valdymo planu, Administravimo taisyklėmis, kitais teisės aktais, reglamentuojančiais saugų Registro duomenų tvarkymą.

II. REGISTRO ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

15. Vadovaujantis Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymu Nr. 1V-247 (Žin., 2007, Nr. 78-3160; 2008, Nr. 127-4866), Registras priskiriamas antrajai informacinių sistemų kategorijai.

16. Registro duomenis sudaro bendrieji, specialieji ir technologiniai duomenys.

17. Registrą sudaro šie posistemiai:

17.1. duomenų registravimo;

17.2. klasifikatorių duomenų tvarkymo;

17.3. sisteminių duomenų tvarkymo;

17.4. naudotojų teisių;

17.5. duomenų mainų;

17.6. ataskaitų formavimo;

17.7. duomenų importavimo;

17.8. duomenų eksportavimo.

18. Registro saugos priemonės parenkamos įvertinus galimus rizikos veiksnius Registro duomenų vientisumui ir prieinamumui.

19. Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja Registro rizikos vertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį Registro rizikos vertinimą.

20. Registro rizikos įvertinimas išdėstomas rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaitą rengia saugos įgaliotinis, atsižvelgęs į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausi rizikos veiksniai yra šie:

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

20.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis Registru Registro duomenims gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugos pažeidimai, vagystės ir kt.);

20.3. nenugalima jėga (darbuotojų praradimas, audros, gaisrai, vandens poveikis, elektros instaliacijos gedimas ir kt.).

21. Lietuvos Respublikos susisiekimo ministras, atsižvelgdamas į rizikos įvertinimo ataskaitą, prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

22. Rizikos veiksnių Registro duomenims, techninei, programinei įrangai, registravimo dokumentams, tikėtinumui vertinti Administracijoje naudojama penkiabalė rizikos veiksnių tikėtinumo ir žalos vertinimo metodika:

22.1. nereikšmingas rizikos veiksnių tikėtinumas, žala – 1 balas;

22.2. mažas rizikos veiksnių tikėtinumas, žala – 2 balai;

22.3. vidutinis rizikos veiksnių tikėtinumas, žala – 3 balai;

22.4. didelis rizikos veiksnių tikėtinumas, žala – 4 balai;

22.5. labai didelis rizikos veiksnių tikėtinumas, žala – 5 balai.

23. Siekiant užtikrinti šiuose nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, kasmet organizuojamas informacinių technologijų saugos atitikties vertinimas, kurio metu:

23.1. įvertinama Saugos nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų ir realios

informacijos saugos atitiktis;

23.2. inventorizuojama Registro techninė ir programinė įranga;

23.3. tikrinama visose Administracijos tarnybinėse stotyse, Registro administratorių bei ne mažiau kaip 50% Registro naudotojų kompiuterinėse darbo vietose įdiegta programinė įranga ir jos sąranka;

23.4. peržiūrima Registro administratoriui ir Registro naudotojams suteiktų teisių atitiktis jų vykdomoms funkcijoms;

23.5. įvertinamas pasirengimas užtikrinti Registro veiklos tęstinumą įvykus saugos incidentui;

23.6. analizuojami rizikos veiksniai, galimos jų pašalinimo arba neigiamo poveikio sumažinimo priemonės ir Saugos nuostatuose reglamentuota tvarka koreguojama rizikos įvertinimo ataskaita.

24. Atlikus Saugos nuostatų 23 punkte nurodytą atitikties vertinimą, saugos įgaliotinis parengia pastebėtų trūkumų šalinimo planą, kurį tvirtina, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminus Lietuvos Respublikos susisiekimo ministras.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

25. Prieigos prie Registro užtikrinimo metodai ir priemonės:

25.1. teisė dirbti su konkrečia elektronine informacija suteikiama konkrečiam Registro naudotojui arba Registro naudotojų grupei;

25.2. pasibaigus valstybės tarnybos (darbo) santykiams, Registro naudotojo teisė naudotis Registru turi būti panaikinta. Registro naudotojui teisė dirbti su konkrečia elektronine informacija turi būti ribojama ar sustabdoma, kai vyksta Registro naudotojo veiklos tyrimas;

25.3. Registro naudotojas turi imtis priemonių, kad su Registro duomenimis negalėtų susipažinti pašaliniai asmenys.

26. Registro duomenims apsaugoti nuo kenksmingos programinės įrangos Administracijoje naudojama antivirusinė programinė priemonė atnaujinama ne rečiau kaip kartą per savaitę.

27. Registro objektų duomenims saugiai rinkti, apdoroti, kaupti, saugoti, teikti kitiems registrams, informacinėms sistemoms, suinteresuotiems juridiniams ir fiziniams asmenims Administracijoje naudojamos programinės ir techninės įrangos naudojimą ribojančios pagrindinės priemonės, kuriose:

27.1. realizuota galimybė Registro naudotojams naudoti tik legalią programinę įrangą;

27.2. realizuota Registro naudotojams prieigos prie Registro duomenų galimybė tik per registravimosi ir slaptažodžių sistemą;

27.3. realizuota galimybė Registro duomenų tvarkytojams ne rečiau kaip kartą per mėnesį, o Registro naudotojams ne rečiau kaip kartą per pusmetį atnaujinti slaptažodžius;

27.4. Registro administratorius savo tapatybę turi patvirtinti slaptažodžiu, kuriam keliami aukštesni reikalavimai negu Registro naudotojų slaptažodžiams;

27.5. Registro naudotojų prieigos valdymas apibrėžtas Registro naudotojų administravimo taisyklėse;

27.6. Registro naudotojas, baigęs darbą, turi imtis priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungti nuo Registro, įjungti ekrano užsklandą su slaptažodžiu, dokumentus padėti į pašaliniams asmenims neprieinamą vietą;

27.7. naudojama Registro administravimo programinės įrangos ugniasienė;

27.8. realizuota galimybė nustatyti prieigos prie Registro duomenų autorius, fiksuoti jų atliktus veiksmus ir juos kaupti;

27.9. realizuota galimybė visas užklausas į Registro duomenų bazę fiksuoti programiniu būdu.

28. Saugos įgaliotinis, Registro administratorius Administracijoje turi organizuoti Registro programinės, techninės įrangos naudojimą ribojančių priemonių įgyvendinimą – periodiškai, ne rečiau kaip kartą per 3 mėnesius, patikrinti, ar nenaudojama nelegali programinė įranga; rasta nelegali programinė įranga turi būti nedelsiant pašalinta.

29. Registro duomenys laikomi tik stacionariuose darbo vietų kompiuteriuose. Bet kokia

prieiga prie Registro duomenų iš nešiojamųjų kompiuterių yra draudžiama. Kompiuteriuose esanti informacija apsaugota operacinės sistemos ir vartotojo vardu bei slaptažodžiu. Kompiuteriuose negali būti jokios svarbios informacijos, išskyrus Registro naudotojo naudojamus darbo dokumentus. Registro duomenys iš kompiuterio pasiekiami tik naudojant Administracijos vidaus tinklą.

30. Viešaisiais telekomunikaciniais tinklais perduodamos elektroninės informacijos konfidencialumas užtikrinamas naudojant virtualų privatų tinklą.

31. Registro duomenų gavimo automatiniu būdu iš kitų informacinių sistemų tvarka nustatyta duomenų teikimo sutartyse.

32. Registro fizinę saugą Radiacinės saugos centre užtikrina šios saugos priemonės: signalizacija, įėjimo kontrolės sistema, apsauginės žaliuzės, stebėjimas vaizdo kamera ir kt.

33. Registrui administruoti naudojamas tarnybinių stočių operacines sistemas, techninę ir programinę įrangą, reikalingą Registro naudotojo funkcijoms vykdyti, diegia ir prižiūri tik Registro administratorius.

34. Registro programinės įrangos diegimą ar atnaujinimą turi atlikti tik Registro administratorius ar įgalioti asmenys.

35. Registro programinės įrangos testavimas turi būti atliekamas naudojant atskirą tam skirtą testavimo aplinką.

36. Už atsarginių Registro duomenų kopijų kūrimo periodiškumą ir saugojimą atsako Registro administratorius. Registro duomenų kopijų saugojimo priemonės, būdai ir vieta, kopijų atkūrimo tvarka, naikinimo tvarka bei asmens, atsakingo už Registro duomenų kopijų kūrimą, saugojimą, atkūrimą, sunaikinimą, teisės ir pareigos išdėstytos Saugaus elektroninės informacijos tvarkymo taisyklėse.

IV. REIKALAVIMAI PERSONALUI

37. Registro objektų duomenims saugiai rinkti, apdoroti, sisteminti, kaupti, saugoti ir teikti kitiems registrams, informacinėms sistemoms, suinteresuotiems juridiniams ir fiziniams asmenims, kitiems duomenų gavėjams gali Registro naudotojai, susipažinę su Lietuvos Respublikos jūrų laivų registro nuostatais, registrų ir informacinių sistemų saugos politiką reglamentuojančiais teisės aktais.

38. Saugos įgaliotinis privalo išmanyti informacijos saugos užtikrinimo principus, savo darbe vadovautis Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, 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), kitais Lietuvos Respublikos teisės aktais, reglamentuojančiais Registro duomenų tvarkymą, standartais bei kitais dokumentais ir būti susipažinęs su esminiais reikalavimais, turėti atitinkamą kvalifikaciją, sugebėti prižiūrėti, kaip įgyvendinama saugos politika.

39. Registro administratorius privalo išmanyti informacijos saugos principus, darbą su kompiuterių tinklais, mokėti užtikrinti jų saugą, taip pat administruoti, prižiūrėti registrų ir informacinių sistemų duomenų bazes, turi būti susipažinęs su Saugos nuostatais ir saugos politiką įgyvendinančiais teisės aktais, taip pat kitomis vidaus ir darbo saugos taisyklėmis.

40. Registro naudotojai turi turėti atitinkamą kvalifikaciją (informacinių technologijų vartotojų kvalifikacijos kursai, pradinis saugaus darbo su duomenimis mokymas, ECDL (Europos kompiuterio vartotojo pažymėjimas) vartotojo sertifikatas ir pan.) ir patirties (dirbant su atitinkamomis operacinėmis sistemomis, taikomosiomis programomis ir pan.).

41. Tvarkyti Registro duomenis gali tik Registro naudotojai, pasirašytinai susipažinę su saugos politiką įgyvendinančiais teisės aktais.

42. Registro naudotojams 1 kartą per metus pateikiamos darbo su Registru instrukcijos. Už instrukcijų pateikimą atsakingas saugos įgaliotinis.

43. Registro naudotojai privalo rūpintis tvarkomų duomenų sauga.

44. Esant elektroninės informacijos saugos incidentui, nenumatytai situacijai, saugos įgaliotinio, Registro administratorių, Registro naudotojų veiksmus reglamentuoja Valdymo planas.

45. Saugos įgaliotinis periodiškai inicijuoja Registro naudotojų mokymą informacijos saugos klausimais, įvairiais būdais informuoja juos apie informacijos saugos problematiką (priminimai elektroniniu paštu, pagal poreikį organizuojami susitikimai su Registro naudotojais, atmintinės naujai priimtiems darbuotojams).

V. REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

46. Registro naudotojų supažindinimą pasirašytinai su šiais Saugos nuostatais ir kitais saugos politiką reglamentuojančiais dokumentais organizuoja bei informuoja Registro naudotojus apie Saugos nuostatų pakeitimus ar kitų saugos politiką įgyvendinančių teisės aktų pripažinimą netekusiais galios, keitimą ar priėmimą saugos įgaliotinis.

47. Saugos įgaliotinis reguliariai įvairiais būdais informuoja Registro naudotojus apie informacijos saugos problematiką.

48. Saugos nuostatai skelbiami Administracijos interneto svetainėje, kiti Registro saugos politiką įgyvendinantys teisės aktai skelbiami Administracijos vidiniame tinklalapyje.

VI. BAIGIAMOSIOS NUOSTATOS

49. Saugos nuostatai ir kiti saugos politiką reglamentuojantys teisės aktai iš esmės peržiūrimi ir prireikus keičiami ne rečiau kaip vieną kartą per metus.

50. Administracija privalo įgyvendinti šiuose Saugos nuostatuose ir kituose teisės aktuose, reglamentuojančiuose Registro duomenų saugų tvarkymą, nustatytas organizacines, technines ir kitas priemones.

51. Duomenys apie Registro duomenų tvarkytojų, Registro administratoriaus atliktus veiksmus su Registro duomenimis saugomi neterminuotai.

52. Registro naudotojai, saugos įgaliotinis ir Registro administratorius raštu įsipareigoja nepažeisti šių Saugos nuostatų ir kitų teisės aktų, reglamentuojančių Registro duomenų saugų tvarkymą.

53. Registro naudotojai, saugos įgaliotinis ir Registro administratorius, pažeidę Saugos nuostatų ar kitų saugos politiką įgyvendinančių teisės aktų reikalavimus, atsako įstatymų nustatyta tvarka.

Priedo pakeitimai:
Nr. 3-547, 2009-11-03, Žin., 2009, Nr. 135-5899 (2009-11-12), i. k. 1092210ISAK0003-547

Lietuvos Respublikos jūrų laivų registro
duomenų saugos nuostatų
priedas

RIZIKOS VEIKSNIAI IR LAIPSNIAI

Nr.	Rizikos veiksniai	Rizikos laipsniai
1.	Atsitiktiniai objektyvūs veiksniai:	
1.1.	Vidiniai rizikos veiksniai:	
1.1.1.	valstybės tarnautojų ir darbuotojų praradimas	Reikšmingas
1.1.2.	atsitiktinės techninės avarijos	Reikšmingas ar kritinis
1.1.3.	purvo, dulkių, magnetinių laukų poveikis	Reikšmingas
1.2.	Išoriniai rizikos veiksmai:	
1.2.1.	audros, gaisrai	Kritinis
1.2.2.	vandens poveikis	Reikšmingas
1.2.3.	elektros instaliacijos degimas	Reikšmingas ar kritinis
1.2.4.	elektros energijos tiekimo sutrikimas	Reikšmingas
2.	Netyčiniai subjektyvūs veiksmai:	
2.1.	Kylantys dėl darbo organizavimo nesklandumų:	
2.1.1.	vidaus tvarkos taisyklių pažeidimai	Reikšmingas
2.1.2.	priežiūros trūkumas	Reikšmingas
2.1.3.	resursų kontrolė	Reikšmingas
2.1.4.	netinkamai paskirstytos naudotojų teisės	Reikšmingas
2.1.5.	programinės įrangos testai	Kritinis
2.1.6.	netinkama duomenų laikmenų priežiūra	Kritinis
2.1.7.	nepakankamas linijų pajėgumas ir apsauga	Reikšmingas
2.1.8.	kompiuterių integravimas į tinklą	Kritinis
2.1.9.	„Windows“ apsaugos trūkumai	Reikšmingas
2.2.	Susiję su techninės ir programinės įrangos gedimu:	
2.2.1.	elektros energijos tiekimo gedimas	Kritinis
2.2.2.	kitų registro informacinės sistemos grandžių veiklos nesklandumai	Reikšmingas
2.2.3.	prisijungimas prie registro informacinės sistemos	Reikšmingas ar kritinis
2.2.4.	programinės įrangos klaidos	Reikšmingas
2.2.5.	duomenų netekimas	Kritinis
2.3.	Kylantys dėl valstybės tarnautojų ir darbuotojų klaidų:	
2.3.1.	netinkamas registro informacinės sistemos naudojimas	Reikšmingas
2.3.2.	įsijungimas į tinklą	Reikšmingas
2.3.3.	duomenų laikmenos	Reikšmingas ar kritinis
2.3.4.	klaidos transportuojant informaciją	Reikšmingas
2.3.5.	duomenų pažeidimas dėl naudotojo klaidos	Reikšmingas ar kritinis
2.3.6.	teisių suteikimas	Reikšmingas
2.3.7.	operacijos su slaptažodžiais	Reikšmingas
3.	Tyčiniai subjektyvūs veiksmai:	
3.1.	Neteisėtas naudojimasis registro informacine sistema	Kritinis
3.2.	Fizinis įsibrovimas į registro informacinę sistemą	Kritinis
3.3.	Įsiterpimas į tinklus	Kritinis
3.4.	Naudotojo teisių pažeidimas	Reikšmingas ar kritinis
3.5.	Duomenų atskleidimas	Reikšmingas ar kritinis
3.6.	Pranešimų tėkmės analizė	Reikšmingas
3.7.	Siuntimo aprašymo protokolai	Reikšmingas
3.8.	Kenkėjiškos kompiuterinės programos	Reikšmingas ar kritinis

_____

Pakeitimai:

1.
Lietuvos Respublikos susisiekimo ministerija, Įsakymas
Nr. 3-547, 2009-11-03, Žin., 2009, Nr. 135-5899 (2009-11-12), i. k. 1092210ISAK0003-547
Dėl Lietuvos Respublikos susisiekimo ministro 2005 m. gruodžio 15 d. įsakymo Nr. 3-568 "Dėl Lietuvos Respublikos jūrų laivų registro duomenų saugos nuostatų patvirtinimo" pakeitimo