LIETUVOS RESPUBLIKOS SUSISIEKIMO MINISTRAS

ĮSAKYMAS
DĖL LIETUVOS SAUGIOS LAIVYBOS ADMINISTRACIJOS TVARKOMŲ REGISTRŲ DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2016 m. vasario 9 d. Nr. 3-48 (1.5 E)
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 7.1 papunkčiu ir 11, 12, 19, 26 punktais:

1. T v i r t i n u Lietuvos saugios laivybos administracijos tvarkomų registrų duomenų saugos nuostatus (pridedama).

2. P a v e d u Lietuvos saugios laivybos administracijai:

2.1. paskirti Lietuvos saugios laivybos administracijos tvarkomų Lietuvos Respublikos jūrų laivų registro, Lietuvos Respublikos vidaus vandenų laivų registro ir Lietuvos Respublikos jūrininkų registro administratorių;

2.2. paskirti Lietuvos saugios laivybos administracijos tvarkomų Lietuvos Respublikos jūrų laivų registro, Lietuvos Respublikos vidaus vandenų laivų registro ir Lietuvos Respublikos jūrininkų registro saugos įgaliotinį;

2.3. ne vėliau kaip per 2 mėnesius nuo šio įsakymo įsigaliojimo dienos parengti ir pateikti Lietuvos Respublikos susisiekimo ministrui tvirtinti saugos politikos įgyvendinamųjų dokumentų projektus.

3. P r i p a ž į s t u netekusiais galios:

3.1. Lietuvos Respublikos susisiekimo ministro 2005 m. gruodžio 15 d. įsakymą Nr. 3-568 „Dėl Lietuvos Respublikos jūrų laivų registro duomenų saugos nuostatų patvirtinimo“ su visais pakeitimais ir papildymais;

3.2. Lietuvos Respublikos susisiekimo ministro 2007 m. kovo 28 d. įsakymą Nr. 3-108 „Dėl Lietuvos Respublikos jūrininkų registro duomenų saugos nuostatų patvirtinimo“ su visais pakeitimais ir papildymais;

3.3. Lietuvos Respublikos susisiekimo ministro 2010 m. birželio 30 d. įsakymą Nr. 3-411 „Dėl Lietuvos Respublikos vidaus vandenų laivų registro duomenų saugos nuostatų patvirtinimo ir Lietuvos Respublikos susisiekimo ministro 2005 m. birželio 6 d. įsakymo Nr. 3-260 „Dėl Lietuvos Respublikos vidaus vandenų laivų registro duomenų saugos nuostatų patvirtinimo“ pripažinimo netekusiu galios“.

Susisiekimo ministras Rimantas Sinkevičius

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2016 m. vasario 2 d. raštu Nr. 1D-665

PATVIRTINTA
Lietuvos Respublikos susisiekimo ministro 2016 m. vasario 9d. įsakymu Nr.3-48 (1.5 E)

LIETUVOS SAUGIOS LAIVYBOS ADMINISTRACIJOS TVARKOMŲ REGISTRŲ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos saugios laivybos administracijos tvarkomų registrų duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Lietuvos saugios laivybos administracijos (toliau – Administracija) tvarkomų Lietuvos Respublikos jūrų laivų registro, Lietuvos Respublikos vidaus vandenų laivų registro ir Lietuvos Respublikos jūrininkų registro (toliau – registrai) elektroninės informacijos saugos politiką.

2. Saugos nuostatuose vartojamos sąvokos atitinka sąvokas, apibrėžtas Saugos nuostatų 18 punkte nurodytuose teisės aktuose.

3. Saugos nuostatai apibrėžia registrų saugos politiką, kuri įgyvendinama pagal šiuos susisiekimo ministro patvirtintus teisės aktus (toliau – saugos politikos įgyvendinamieji dokumentai):

3.1. Saugaus elektroninės informacijos tvarkymo taisykles;

3.2. Veiklos tęstinumo valdymo planą;

3.3. Naudotojų administravimo taisykles.

4. Saugos nuostatų reikalavimai taikomi tvarkant:

4.1. Lietuvos Respublikos jūrų laivų registrą;

4.2. Lietuvos Respublikos vidaus vandenų laivų registrą;

4.3. Lietuvos Respublikos jūrininkų registrą.

5. Saugos nuostatų reikalavimai taikomi tvarkant Saugos nuostatų 4 punkte nurodytų registrų duomenis ir yra privalomi valstybės tarnautojams, darbuotojams, dirbantiems pagal darbo sutartis, kitiems asmenims, kuriems suteiktos bet kokios registrų naudotojų teisės.

6. Elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

6.1. elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

6.2. registrų elektroninei informacijai tvarkyti naudojamos techninės ir programinės įrangos ir duomenų tvarkymo kontrolė;

6.3. fizinė elektroninės informacijos apdorojimo priemonių (patalpų, tarnybinių stočių, elektroninės informacijos perdavimo įrangos, programinės įrangos) apsauga;

6.4. registrų veiklos tęstinumo užtikrinimas;

6.5. registrų naudotojų mokymas;

6.6. asmens duomenų apsauga.

7. Elektroninės informacijos saugumo tikslai:

7.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti elektroninę informaciją registruose;

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

8. Saugos nuostatai taikomi registrų valdytojai – Lietuvos Respublikos susisiekimo ministerijai (Gedimino pr. 17, Vilnius) ir registrų tvarkytojai – Administracijai (J. Janonio g. 24, Klaipėda), taip pat saugos įgaliotiniui, administratoriui ir naudotojams.

9. Registrų valdytojo funkcijos:

9.1. metodiškai vadovauti registrų tvarkytojui, koordinuoti registrų tvarkytojo veiklą ir registrų funkcionavimą;

9.2. atlikti elektroninės informacijos saugos reikalavimų laikymosi priežiūrą;

9.3. nagrinėti registrų tvarkytojo pasiūlymus dėl registrų elektroninės informacijos saugos tobulinimo ir priimti dėl jų sprendimus;

9.4. priimti įsakymus dėl registrų elektroninės informacijos saugumo užtikrinimo;

9.5. užtikrinti spartų ir veiksmingą registrų pokyčių valdymo planavimą;

9.6. prireikus tvirtinti rizikos įvertinimo ir rizikos valdymo priemonių planą;

9.7. prireikus tvirtinti registrų informacinių technologijų saugos atitikties vertinimo metu pastebėtų trūkumų šalinimo planą;

9.8. atlikti kitas Saugos nuostatuose ir kituose teisės aktuose nustatytas funkcijas.

10. Registrų tvarkytojo funkcijos:

10.1. užtikrinti registrų nepertraukiamą veikimą;

10.2. tvarkyti duomenis ir užtikrinti registrų duomenų saugą ir saugų duomenų perdavimą kompiuterių tinklais (automatiniu būdu);

10.3. teikti pasiūlymus registrų valdytojui, kaip tobulinti registrų duomenų saugą;

10.4. užtikrinti registrų valdytojo priimtų teisės aktų ir rekomendacijų tinkamą įgyvendinimą;

10.5. ne rečiau kaip kartą per metus organizuoti saugos dokumentų persvarstymą (peržiūrėjimą);

10.6. organizuoti registrų naudotojams mokomuosius ir pažintinius kursus registrų elektroninės informacijos tvarkymo klausimais;

10.7. atlikti kitas Saugos nuostatuose ir kituose teisės aktuose nustatytas funkcijas.

11. Už elektroninės informacijos saugą pagal kompetenciją atsako registrų valdytojas ir registrų tvarkytojas.

12. Registrų valdytojas atsako už saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą.

13. Registrų tvarkytojas atsako už tai, kad būtų įgyvendinamos ir užtikrinamos reikiamos administracinės, techninės ir organizacinės saugos priemonės ir kad būtų laikomasi Saugos nuostatų ir saugos politikos įgyvendinamųjų dokumentų.

14. Registrų saugos įgaliotinio (toliau – saugos įgaliotinis), koordinuojančio ir prižiūrinčio registrų saugos politikos įgyvendinimą, funkcijos:

14.1. teikti registrų valdytojo ar tvarkytojo, jeigu jis paskyrė saugos įgaliotinį, vadovui pasiūlymus dėl:

14.1.1. administratorių paskyrimo ir reikalavimų administratoriams nustatymo;

14.1.2. informacinių technologijų saugos atitikties vertinimo, atsižvelgiant į vidaus reikalų ministro nustatytas metodines priemones, atlikimo;

14.2. teikti registro valdytojo vadovui pasiūlymus dėl saugos dokumentų priėmimo, keitimo;

14.3. informuoti registrų valdytojo vadovą apie registrų saugos problemas;

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

14.5. teikti registrų administratoriui ir registrų naudotojams privalomus vykdyti nurodymus ir pavedimus dėl saugos politikos įgyvendinimo;

14.6. organizuoti registrų rizikos ir informacinių technologijų saugos atitikties įvertinimą;

14.7. periodiškai organizuoti registrų naudotojų mokymus elektroninės informacijos saugos klausimais, įvairiais būdais informuoti juos apie elektroninės informacijos saugos problemas;

14.8. atlikti kitas Saugos nuostatuose, kituose teisės aktuose nustatytas ir Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame 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“, saugos įgaliotiniui priskirtas funkcijas.

15. Saugos įgaliotinis negali atlikti registrų administratoriaus funkcijų.

16. Administratoriaus, vykdančio registrų priežiūrą, funkcijos:

16.1. suteikti teisę registrų tvarkytojo darbuotojams naudotis duomenimis priskirtoms funkcijoms atlikti;

16.2. atlikti registrų naudotojų teisų valdymą;

16.3. administruoti registrų komponentus (kompiuterius, operacines sistemas, duomenų bazių valdymo sistemas, taikomųjų programų sistemas, ugniasienes, informacijos perdavimo tinklus ir kitus komponentus), nustatyti pažeidžiamas vietas ir saugos reikalavimų atitiktį, vykdyti stebėseną;

16.4. teikti saugos įgaliotiniui informaciją apie registrų komponentų būklę;

16.5. registruoti registrų saugos incidentus ir informuoti apie juos saugos įgaliotinį, teikti siūlymus dėl minėtų incidentų šalinimo;

16.6. ne rečiau kaip kartą per metus ir (arba) atlikus registrų pakeitimus tikrinti registrų komponentų sąranką ir registrų būsenos rodiklius;

16.7. vykdyti saugos įgaliotinio nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu;

16.8. atsakyti už registrų funkcionavimą užtikrinančios techninės ir programinės įrangos, infrastruktūros bei informacinių technologijų paslaugų administravimą, registrų naudotojų ir registravimo vardų skyrimą, prieigos prie registrų teisių nustatymą;

16.9. atsakyti už priskirtų registrų komponentų (kompiuterizuotų darbo vietų (toliau – KDV), tarnybinių stočių, operacinių sistemų, duomenų bazių, užkardų, duomenų perdavimo tinklų) administravimą, registrų komponentų sąrankos aprašymo dokumentacijos parengimą ir atnaujinimą, saugos priemonių registrų pažeidžiamoms vietoms parinkimą ir jų atitiktį Saugos nuostatų ir kitų saugos dokumentų reikalavimams;

16.10. pagal kompetenciją rengti pasiūlymus registrų tvarkytojui ir saugos įgaliotiniui dėl registrų palaikymo, priežiūros ir elektroninės informacijos saugos;

16.11. atlikti kitas Saugos nuostatuose ir kituose saugos dokumentuose registrų administratoriui priskirtas funkcijas ir kitus registrų valdytojo nurodymus ir pavedimus, susijusius su registrų saugos užtikrinimu.

17. Registrų naudotojai, vadovaudamiesi registrų valdytojo patvirtintais posistemių ir informacinių sistemų nuostatais, Saugos nuostatais, Naudotojų administravimo taisyklėmis, Saugaus elektroninės informacijos tvarkymo taisyklėmis ir pareigybių aprašymais, privalo:

17.1. naudotis registrais tik su tiesioginių funkcijų atlikimu susijusiais tikslais;

17.2. užtikrinti duomenų tvarkymo teisėtumą;

17.3. informuoti saugos įgaliotinį, administratorių apie elektroninės informacijos saugos incidentus, registrų darbo sutrikimus;

17.4. vykdyti kitas Saugos nuostatuose ir saugos politikos įgyvendinamuosiuose dokumentuose nustatytas funkcijas ir kitus registrų valdytojo, saugos įgaliotinio ir administratoriaus nurodymus, susijusius su registrų naudojimu ir sauga.

18. Teisės aktai, kuriais vadovaujamasi tvarkant registrų elektroninę informaciją ir užtikrinant jos saugą:

18.1. Lietuvos Respublikos kibernetinio saugumo įstatymas;

18.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

18.3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

18.4. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas, patvirtintas 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“;

18.5. Lietuvos Respublikos jūrų laivų registro nuostatai, patvirtinti Lietuvos Respublikos Vyriausybės 2004 m. spalio 21 d. nutarimu Nr. 1318 „Dėl Lietuvos Respublikos jūrų laivų registro“;

18.6. Lietuvos Respublikos vidaus vandenų laivų registro nuostatai, patvirtinti Lietuvos Respublikos Vyriausybės 2004 m. lapkričio 11 d. nutarimu Nr. 1435 „Dėl Lietuvos Respublikos vidaus vandenų laivų registro“;

18.7. Lietuvos Respublikos jūrininkų registro nuostatai, patvirtinti Lietuvos Respublikos Vyriausybės 2006 m. gruodžio 6 d. nutarimu Nr. 1212 „Dėl Lietuvos Respublikos jūrininkų registro“;

18.8. 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“;

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

18.10. Lietuvos standartai 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“ standartai, reguliuojantys saugų informacinės sistemos duomenų tvarkymą;

18.11. kiti teisės aktai, reglamentuojantys registrų duomenų tvarkymo teisėtumą, registrų tvarkytojo veiklą ir duomenų saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

19. Atsižvelgiant į registrų duomenų savybių (vientisumo, konfidencialumo ir prieinamumo) įtaką Susisiekimo ministerijos veiklai, registruose, nurodytuose Saugos nuostatų 4 punkte, vadovaujantis 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 „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“ (toliau – Informacijos svarbos nustatymo gairių aprašas), 4.3 ir 4.4 papunkčiuose nurodytais kriterijais, saugoma informacija priskiriama svarbios elektroninės informacijos kategorijai.

20. Atsižvelgiant į registrų duomenų savybių (vientisumo, konfidencialumo ir prieinamumo) įtaką Susisiekimo ministerijos veiklai, registrai, nurodyti Saugos nuostatų 4 punkte, vadovaujantis Informacijos svarbos nustatymo gairių aprašo 5 punkte nurodytais kriterijais, priskiriami antrajai informacinių sistemų kategorijai.

21. Registrų saugos priemonės parenkamos įvertinus galimus rizikos veiksnius registrų duomenų vientisumui, konfidencialumui ir prieinamumui. Pasirenkant saugos priemones, prioritetas teikiamas toms priemonėms, kurioms įdiegti reikia mažiausiai sąnaudų ir gaunamas didžiausias poveikis.

22. Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija.

Saugumo technika“ grupės standartus ir taikydamas pasaulyje pripažintas metodikas, kasmet organizuoja registrų rizikos vertinimą, o prireikus ir neeilinį rizikos vertinimą. Prireikus, registrų valdytojo ar tvarkytojo pavedimu registrų rizikos vertinimui atlikti gali būti perkamos rizikos vertinimo paslaugos.

23. Registrų rizikos veiksnių įvertinimas pateikiamas rizikos įvertinimo ataskaitoje, kuri rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausi rizikos veiksniai yra šie:

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

23.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugos pažeidimai, vagystės ir kt.);

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

24. Rizikos veiksnių registrų elektroninei informacijai, techninei, programinei įrangai, registravimo dokumentams, tikėtinumui vertinti turi būti naudojama penkių balų rizikos veiksnių tikėtinumo ir žalos vertinimo metodika:

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

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

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

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

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

25. Rizikos vertinimo metu atliekamos veiklos:

25.1. registrus sudarančių informacinių išteklių inventorizacija;

25.2. įtakos registrų veiklai vertinimas;

25.3. grėsmės ir pažeidimų analizė;

25.4. liekamosios rizikos vertinimas.

26. Registrų rizikos įvertinimo ataskaita pateikiama registrų valdytojo at registrų tvarkytojo, jeigu ji paskyrė saugos įgaliotinį, vadovui.

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

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

28.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

28.2. informacijos saugos priemonės diegimo kainos turi atitikti saugomos informacijos vertę;

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

29. Siekiant užtikrinti Saugos nuostatuose ir saugos politikos įgyvendinamuosiuose dokumentuose išdėstytų nuostatų įgyvendinimo organizavimą ir kontrolę, ne rečiau kaip kartą per dvejus metus saugos įgaliotinis organizuoja informacinių technologijų saugos atitikties įvertinimą, kurio metu:

29.1. įvertinama esamos elektroninės informacijos saugos padėties atitiktis Saugos nuostatų Bendrųjų elektroninės informacijos saugos reikalavimų ir saugos politikos įgyvendinamųjų dokumentų reikalavimams;

29.2. inventorizuojama registrų techninė ir programinė įranga;

29.3. patikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų registrų naudotojų KDV, visose Administracijos tarnybinėse stotyse įdiegta programinė įranga ir jos sąranka;

29.4. patikrinama (įvertinama) registrų naudotojams suteiktų teisių atitiktis jų vykdomoms funkcijoms;

29.5. įvertinamas pasirengimas užtikrinti registrų veiklos tęstinumą įvykus elektroninės informacijos saugos incidentui.

30. Atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama registrų valdytojo ar registrų tvarkytojo, jeigu jis paskyrė saugos įgaliotinį, vadovui, ir pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato registrų valdytojas.

31. Neeilinis registrų rizikos vertinimas turi būti atliekamas:

31.1. įvykus pokyčiams registrų techninėje ar programinėje įrangoje, kurie galėtų turėti įtakos registrų veikimui;

31.2. paaiškėjus naujoms tendencijoms informacinių technologijų saugos srityje, dėl kurių kiltų grėsmė registrų techninei, programinei įrangai ar registruose laikomiems duomenims;

31.3. po saugos incidento, kurio metu būtų sutrikdyta registrų veikla, sugadinti ar prarasti registrų duomenys.

32. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano, registrų informacinių technologijų saugos atitikties vertinimo ataskaitos ir pastebėtų trūkumų šalinimo plano kopijas registrų valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2012 m. spalio 16 d. įsakymu Nr. 1V-740 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

33. Pokyčiai, galintys sutrikdyti ar sustabdyti registrų darbą, turi būti suderinti su registrų valdytojo vadovu ar jo įgaliotu asmeniu.

34. Pokyčiai, galintys daryti neigiamą įtaką elektroninės informacijos konfidencialumui, vientisumui ar prieinamumui, turi būti patikrinti bandomojoje aplinkoje, kurioje nėra konfidencialių ir asmens duomenų ir kuri atskirta nuo eksploatuojamų registrų.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

35. Programinės įrangos, skirtos registrams ir KDV nuo kenksmingos programinės įrangos apsaugoti, naudojimo nuostatos:

35.1. visose KDV, kuriose dirbama su registrų duomenimis, privalo būti naudojama programinė įranga, skirta KDV nuo kenksmingos programinės įrangos apsaugoti;

35.2. registrų duomenims ir KDV nuo kenksmingos programinės įrangos apsaugoti registrų valdytojo ir tvarkytojo įstaigose turi būti naudojamos legalios programinės priemonės;

35.3. registrų naudotojų kompiuteriuose naudojama įranga, skirta KDV nuo kenksmingos programinės įrangos apsaugoti, turi apsaugoti ir elektroninio pašto programinę įrangą nuo nepageidaujamo pašto ar kenksmingų programų pateikimo į KDV;

35.4. registrų naudotojų kompiuteriuose esanti programinė įranga, skirta registrams ir KDV nuo kenksmingos programinės įrangos apsaugoti, turi būti atnaujinama automatiniu būdu ne rečiau kaip kas trys dienos;

35.5. atsiradus požymių, kad KDV yra kenksmingų programų, turi būti patikrinami visi KDV standieji diskai, naudojama programinė įranga, skirta registrams ir KDV nuo kenksmingos programinės įrangos apsaugoti;

35.6. KDV esančios programinės įrangos, skirtos registrams ir KDV nuo kenksmingos programinės įrangos apsaugoti, nustatymai turi būti parinkti pagal rekomenduojamus tokios

programinės įrangos gamintojų reikalavimus arba pagal vidinio kompiuterių tinklo administratoriaus rekomendacijas;

35.7. registrų programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims.

36. Programinės įrangos, įdiegtos KDV ir tarnybinėse stotyse, naudojimo nuostatos:

36.1. registrų naudotojams draudžiama diegti ir naudoti bet kokią programinę įrangą, keisti sistemos, kompiuterio ar programinės įrangos sistemų nustatymus; programinę įrangą, reikalingą registrų naudotojo funkcijoms atlikti, KDV diegia, atnaujina, kontroliuoja ir prižiūri tik administratorius; kiti asmenys (paslaugų teikėjų specialistai) gali diegti programinę įrangą tik prižiūrint administratoriams;

36.2. diegti ir naudoti programinę įrangą, nesusijusią su registrų valdytojo ar tvarkytojo veikla ar registrų naudotojo atliekamomis funkcijomis (žaidimų, bylų siuntimo, internetinių pokalbių programas ir kt.), draudžiama.

37. Registrų naudotojai turi vadovautis „švaraus stalo“ politika:

37.1. nors trumpam paliekant KDV, privaloma įjungti slaptažodžiu apsaugotą ekrano užsklandą;

37.2. baigus darbą, reikia uždaryti programų langus ir tinkamai išjungti kompiuterį;

37.3. baigus darbą nepalikti ant stalo dokumentų ir duomenų laikmenų, sudėti juos į stalčius, spintas ar lentynas;

37.4. dokumentų, kuriuose pateikiama ypač svarbi informacija, spausdinimą inicijavęs asmuo iš spausdintuvų juo turi išimti nedelsdamas;

37.5. nebereikalingi ypač svarbūs dokumentai turi būti ne išmetami, o sunaikinami dokumentų naikikliu.

38. Kompiuterių tinklo filtravimo įrangos pagrindinės naudojimo nuostatos:

38.1. registrų naudotojų prieiga prie kitų valstybės institucijų kompiuterinių tinklų ar interneto turi būti apsaugota užkardomis;

38.2. interneto turinys turi būti kontroliuojamas nepraleidžiant nepageidaujamos informacijos;

38.3. už kompiuterių tinklo filtravimo įrangos administravimo koordinavimą ir priežiūrą atsakingas administratorius.

39. Leistinos kompiuterių naudojimo ribos:

39.1. stacionarius kompiuterius leidžiama naudoti tik registrų valdytojo ir tvarkytojo patalpose;

39.2. registrų naudotojai kompiuterius naudoja tik tarnybinėms funkcijoms atlikti;

39.3. registrų naudotojai, tarnybinėms funkcijoms atlikti naudojantys nešiojamuosius kompiuterius, išnešdami juos iš registrų valdytojo ir tvarkytojo patalpų, norėdami registrų duomenis perduoti kompiuterių tinklais ne savo darbo vietoje, turi naudoti duomenų šifravimą, papildomą registrų naudotojo tapatybės patvirtinimą, rakinimo įrenginį, nešiojamojo kompiuterio pagrindinė įvesties ir išvesties sistema (BIOS) turi būti apsaugota slaptažodžiu ir nurodytas kietasis diskas kaip pirminis paleidimo įrenginys.

40. Užtikrinant saugų elektroninės informacijos teikimą kitoms valstybės institucijoms ir (ar) gavimą iš jų, naudojamas ribotas virtualus privatus tinklas arba Saugus valstybinis duomenų perdavimo tinklas (toliau – SVDPT). Elektronine informacija keičiamasi per saugųjį HTTP protokolą (HTTPS) žiniatinklio paslaugų metodu (XML formatu) arba duomenų bazių užklausomis. Duomenys teikiami ir (ar) gaunami automatiniu būdu tik pagal duomenų teikimo sutartyje nustatytas specifikacijas ir sąlygas.

41. Registrų naudotojų kompiuterių tinklas turi tenkinti SVDPT saugaus organizavimo, valdymo ir SVDPT naudotojų prijungimo reikalavimus, nustatytus 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“.

42. Pagrindiniai atsarginių duomenų kopijų darymo ir atkūrimo reikalavimai:

42.1. registrų atsarginės duomenų kopijos turi būti daromos periodiškai (visų duomenų kopija – ne rečiau kaip vieną kartą per savaitę);

42.2. periodiškai (ne rečiau kaip kartą per metus) turi būti bandoma atkurti duomenis iš atsarginių duomenų kopijų; bandymo eiga ir rezultatai įforminami kopijų darymo žurnale;

42.3. atsarginės kopijos turi būti saugomos atskirai nuo darbinės registrų infrastruktūros; registrų atsarginės kopijos gali būti saugomos trečiųjų šalių debesijos infrastruktūroje (angl. *cloud infrastructure*), jeigu minima infrastruktūra yra NATO šalyje ir jeigu minėtos paslaugos teikėjas gali užtikrinti tinkamą kopijų saugumą;

42.4. už atsarginių duomenų kopijų darymą ir saugojimą yra atsakingi administratoriai, vykdantys registrų priežiūrą.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

43. Saugos įgaliotinis privalo išmanyti informacijos saugos užtikrinimo principus ir priemones (informacijos, konfidencialumo, vientisumo, pasiekiamumo apsaugos principus, organizacines apsaugos, technines apsaugos priemones, apsaugos informacinių priemonių visumą), savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 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.

44. 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 įrenginio, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo administracinės nuobaudos paskyrimo praėję mažiau kaip vieneri metai.

45. Registrų administratorius privalo išmanyti pagrindinius saugos politikos principus, darbą su duomenų perdavimo tinklais, užtikrinti jų saugumą, turėti sisteminių programinių priemonių (*Windows, Linux, Oracle*) administravimo ir priežiūros patirties.

46. Registrų naudotojai turi turėti atitinkamą kvalifikaciją (darbo su kompiuteriu įgūdžiai, informacinių technologijų vartotojų kvalifikacijos kursai, pradinis saugaus darbo su elektronine informacija mokymas, ECDL (Europos kompiuterio vartotojo pažymėjimas) vartotojo sertifikatas ar pan.), patirties (darbo su atitinkamomis operacinėmis sistemomis, taikomosiomis programomis ir pan.), mokėti tvarkyti duomenis registrų nuostatų ir duomenų tvarkymo taisyklių nustatyta tvarka ir būti pasirašytinai susipažinę su šiais Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais.

47. Registrų naudotojai privalo rūpintis tvarkomų duomenų saugumu: vadovaudamiesi saugos politikos įgyvendinamaisiais dokumentais, nuolat rūpintis registrų sauga, o pastebėję pažeidimų, neveikiančias duomenų saugos užtikrinimo priemones, nusikalstamos veiklos požymių privalo nedelsdami apie tai pranešti registrų administratoriams arba saugos įgaliotiniui.

48. Registrų naudotojų veiksmus, esant nenumatytai situacijai, reglamentuoja registrų veiklos tęstinumo valdymo planas.

49. Registrų valdytojas kartu su tvarkytoju turi užtikrinti tinkamą saugos įgaliotinio, administratorių ir registrų naudotojų kvalifikacijos tobulinimą.

50. Saugos įgaliotinis periodiškai (ne rečiau kaip kartą per 12 mėnesių) organizuoja registrų administratorių ir naudotojų mokymus, taip pat įvairiomis priemonėmis (pvz., elektroniniu paštu, per teminius seminarus, pateikdamas atmintines naujai priimtiems darbuotojams) informuoja juos apie kilusias informacijos saugos problemas ir, jei žinoma, galimas taikytinas prevencines ar kitas reagavimo priemones.

V SKYRIUS
REGISTRŲ NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

51. Tvarkyti registrų duomenis gali tik registrų naudotojai, pasirašytinai susipažinę su šiais Saugos nuostatais, saugos politikos įgyvendinamaisiais dokumentais ir atsakomybe už saugos dokumentų nuostatų pažeidimus ir sutikę laikytis saugos dokumentuose nustatytų reikalavimų.

52. Saugos nuostatai skelbiami Administracijos interneto svetainėje, kiti registrų saugos politikos įgyvendinamieji dokumentai skelbiami Administracijos interneto svetainės skyriaus „Vidinė zona“ srityje „Duomenų sauga“.

53. Registrų naudotojų ir administratoriaus supažindinimą su Saugos nuostatais, saugos politikos įgyvendinamaisiais dokumentais ir atsakomybe už juose nustatytų reikalavimų nesilaikymą organizuoja saugos įgaliotinis.

54. Registrų saugos įgaliotinis atsakingas už tai, kad registrų naudotojai būtų raštu informuoti apie Saugos nuostatų ir saugos politikos įgyvendinamųjų dokumentų priėmimą, pakeitimą ar pripažinimą netekusiais galios.

55. Pakartotinai su Saugos nuostatais ir saugos politikos įgyvendinamaisiais dokumentais registrų naudotojai pasirašytinai supažindinami tik iš esmės pasikeitus registrų arba informacijos saugą reglamentuojamiems dokumentams.

56. Saugos įgaliotinis:

56.1. supažindina su informacija apie Saugos nuostatų ar saugos politikos įgyvendinamųjų dokumentų priėmimą, keitimą ar pripažinimą netekusiais galios – per 10 darbo dienų nuo teisės akto priėmimo, keitimo ar pripažinimo netekusiu galios (informacija pateikiama Administracijos interneto svetainės skyriaus „Vidinė zona“ srityje „Duomenų sauga“);

56.2. supažindina su informacija apie kvalifikacijos tobulinimą duomenų saugos klausimais, saugaus darbo su duomenimis būdais – žodžiu, elektroniniu paštu ar telefonu, pildydamas ir atnaujindamas Administracijos interneto svetainės Vidinės zonos skilties „Duomenų sauga“ informaciją;

56.3. rengia ir atnaujina atmintines saugos klausimais pagal poreikį, bet ne rečiau kaip kartą per metus.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

57. Saugos nuostatai ir kiti saugos politikos įgyvendinamieji teisės aktai skelbiami registrų tvarkytojo interneto svetainėje.

58. Registrų valdytojas saugos dokumentus gali keisti savo arba saugos įgaliotinio iniciatyva. Keičiami saugos dokumentai turi būti derinami su Lietuvos Respublikos vidaus reikalų ministerija. Keičiami saugos dokumentai gali būti nederinami su Lietuvos Respublikos vidaus reikalų ministerija tais atvejais, kai atliekami tik redakciniai ar nedideli nustatyto teisinio reguliavimo esmės ar saugos politikos nekeičiantys pakeitimai arba taisoma teisės technika.

59. Registrų tvarkytojas saugos dokumentus turi persvarstyti (peržiūrėti) ne rečiau kaip kartą per kalendorinius metus. Saugos dokumentai turi būti persvarstomi (peržiūrimi) atlikus

rizikos įvertinimą ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems registrų tvarkytojo pokyčiams.

_____