Suvestinė redakcija nuo 2024-04-20

Įsakymas paskelbtas: TAR 2016-02-09, i. k. 2016-02544

Nauja redakcija nuo 2024-04-20:
Nr. 3-138, 2024-04-19, paskelbta TAR 2024-04-19, i. k. 2024-07254

LIETUVOS RESPUBLIKOS SUSISIEKIMO MINISTRAS

ĮSAKYMAS DĖL LIETUVOS RESPUBLIKOS JŪRININKŲ REGISTRO, LIETUVOS RESPUBLIKOS JŪRŲ LAIVŲ REGISTRO IR LIETUVOS RESPUBLIKOS VIDAUS VANDENŲ LAIVŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

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

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 15 straipsniu, Lietuvos Respublikos kibernetinio saugumo įstatymo 11 straipsnio 1 dalies 5 punktu ir 22 straipsnio 2 dalimi, įgyvendindamas 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 ir Saugos dokumentų turinio gairių aprašo patvirtinimo“, 7, 11, 19 ir 26 punktus:

1. T v i r t i n u pridedamus:

1.1. Lietuvos Respublikos jūrininkų registro duomenų saugos nuostatus;

1.2. Lietuvos Respublikos jūrų laivų registro duomenų saugos nuostatus;

1.3. Lietuvos Respublikos vidaus vandenų laivų registro duomenų saugos nuostatus.

2. P a v e d u Lietuvos transporto saugos administracijai:

2.1. per 14 darbo dienų nuo šio įsakymo įsigaliojimo dienos paskirti:

2.1.1. Lietuvos Respublikos jūrininkų registro saugos įgaliotinį, duomenų valdymo įgaliotinį, administratorių, asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą, ir asmenį, kontroliuojantį informacinių technologijų paslaugų teikėjo darbą;

2.1.2. Lietuvos Respublikos jūrų laivų registro saugos įgaliotinį, duomenų valdymo įgaliotinį, administratorių, asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą, ir asmenį, kontroliuojantį informacinių technologijų paslaugų teikėjo darbą;

2.1.3. Lietuvos Respublikos vidaus vandenų laivų registro saugos įgaliotinį, duomenų valdymo įgaliotinį, administratorių, asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą, ir asmenį, kontroliuojantį informacinių technologijų paslaugų teikėjo darbą;

2.2. per 20 darbo dienų nuo šio įsakymo įsigaliojimo dienos pateikti Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos paskirtų asmenų ar padalinių, atsakingų už kibernetinio saugumo organizavimą ir užtikrinimą, kontaktinę informaciją;

2.3. per 3 mėnesius nuo šio įsakymo įsigaliojimo dienos pateikti susisiekimo ministrui:

2.3.1. Lietuvos Respublikos jūrininkų registro saugaus elektroninės informacijos tvarkymo taisyklių projektą;

2.3.2. Lietuvos Respublikos jūrininkų registro veiklos tęstinumo valdymo plano projektą;

2.3.3. Lietuvos Respublikos jūrininkų registro naudotojų administravimo taisyklių projektą;

2.3.4. Lietuvos Respublikos jūrų laivų registro saugaus elektroninės informacijos tvarkymo taisyklių projektą;

2.3.5. Lietuvos Respublikos jūrų laivų registro veiklos tęstinumo valdymo plano projektą;

2.3.6. Lietuvos Respublikos jūrų laivų registro naudotojų administravimo taisyklių projektą;

2.3.7. Lietuvos Respublikos vidaus vandenų laivų registro saugaus elektroninės informacijos tvarkymo taisyklių projektą;

2.3.8. Lietuvos Respublikos vidaus vandenų laivų registro veiklos tęstinumo valdymo plano projektą;

2.3.9. Lietuvos Respublikos vidaus vandenų laivų registro naudotojų administravimo taisyklių projektą.

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 9 d. įsakymu Nr. 3-48(1.5 E)
(Lietuvos Respublikos susisiekimo ministro
2024 m. balandžio 19 d. įsakymo Nr. 3-138
redakcija)

LIETUVOS RESPUBLIKOS JŪRININKŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos jūrininkų registro duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Lietuvos Respublikos jūrininkų registro (toliau – registras) elektroninės informacijos saugos politiką ir kibernetinio saugumo politiką (toliau – saugos politika), kurių tikslas – nustatyti ir įgyvendinti organizacines, administracines, technines ir kitas priemones, suteikiančias galimybę saugiai tvarkyti registro duomenis ir užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo netyčinio ar neteisėto sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jos.

2. Saugos nuostatuose vartojamos sąvokos suprantamos taip, kaip jos yra apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, 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 ir Saugos dokumentų turinio gairių aprašo patvirtinimo“ (toliau – Aprašas).

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

3.1. Lietuvos Respublikos jūrininkų registro saugaus elektroninės informacijos tvarkymo taisyklės;

3.2. Lietuvos Respublikos jūrininkų registro naudotojų administravimo taisyklės;

3.3. Lietuvos Respublikos jūrininkų registro veiklos tęstinumo valdymo planas.

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

5. Registro elektroninės informacijos saugos ir kibernetinio saugumo (toliau – registro elektroninės informacijos sauga) užtikrinimo tikslai:

5.1. sudaryti sąlygas saugiai automatizuotomis priemonėmis tvarkyti registro elektroninę informaciją;

5.2. užtikrinti registro elektroninės informacijos patikimumą, konfidencialumą, prieinamumą, vientisumą ir tinkamą techninės, programinės ir ryšių įrangos funkcionavimą;

5.3. vykdyti elektroninės informacijos saugos ir kibernetinių incidentų (toliau – saugos incidentai), asmens duomenų saugumo pažeidimų prevenciją, reaguoti į saugos incidentus, asmens duomenų saugumo pažeidimus ir juos operatyviai suvaldyti.

6. Registro elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

6.1. registro elektroninei informacijai tvarkyti naudojamos techninės ir programinės įrangos kontrolė;

6.2. registro elektroninės informacijos tvarkymo kontrolė;

6.3. saugaus darbo su registro elektronine informacija kontrolė;

6.4. fizinė registro elektroninės informacijos tvarkymo priemonių (tarnybinių stočių, informacijos perdavimo įrangos, programinės įrangos) ir patalpų apsauga;

6.5. registro veiklos tęstinumas.

7. Registro valdytoja ir asmens duomenų valdytoja yra Lietuvos Respublikos susisiekimo ministerija, esanti adresu Gedimino pr. 17, 01103 Vilnius (toliau – registro valdytojas). Registro tvarkytoja ir asmens duomenų tvarkytoja yra Lietuvos transporto saugos administracija, esanti adresu Švitrigailos g. 42, 03209 Vilnius (toliau – Administracija).

8. Saugos nuostatais privalo vadovautis:

8.1. Administracijos valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis, registro saugos įgaliotinis (toliau – saugos įgaliotinis), registro administratorius, asmuo ar padalinys, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą (toliau – kibernetinio saugumo vadovas), registro duomenų valdymo įgaliotinis (toliau – duomenų valdymo įgaliotinis);

8.2. Administracijos Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka išrinkto juridinio asmens ar asmenų (asmenų grupės), kuriems Valstybės informacinių išteklių valdymo įstatymo 39 straipsnyje nustatytomis sąlygomis ir tvarka perduotos registro ir (ar) jo infrastruktūros priežiūros funkcijos (toliau – registro paslaugos teikėjas (-ai)), darbuotojai;

8.3. kiti subjektai, kuriems taikomi Saugos nuostatų reikalavimai.

9. Registro valdytojas atlieka šias funkcijas:

9.1. formuoja registro saugos politiką ir organizuoja jos įgyvendinimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą;

9.2. tvirtina registro saugos dokumentus, prižiūri ir kontroliuoja, kad registras būtų tvarkomas vadovaujantis šiais dokumentais, registro nuostatais ir kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą;

9.3. nagrinėja Administracijos pasiūlymus dėl registro elektroninės informacijos saugos tobulinimo ir priima dėl jų sprendimus;

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

9.5. atsižvelgdamas į kibernetinio saugumo atitikties reikalavimams vertinimo ataskaitą, prireikus tvirtina nustatytų trūkumų šalinimo planą;

9.6. priima sprendimą atlikti registro informacinių technologijų saugos atitikties vertinimą;

9.7. prireikus tvirtina registro informacinių technologijų saugos atitikties vertinimo metu pastebėtų trūkumų šalinimo planą;

9.8. įgyvendina registro pokyčius ir plėtrą;

9.9. pagal kompetenciją užtikrina registro elektroninės informacijos saugos priemones;

9.10. paveda Administracijai paskirti saugos įgaliotinį, duomenų valdymo įgaliotinį, registro administratorių, kibernetinio saugumo vadovą;

9.11. vykdo kitas registro saugos dokumentų ir kitų teisės aktų, reglamentuojančių saugų elektroninės informacijos tvarkymą, nustatytas funkcijas.

10. Administracija atlieka šias funkcijas:

10.1. įgyvendina reikiamas administracines, technines ir organizacines saugos priemones, užtikrina registro saugos reikalavimų atitiktį Saugos nuostatams ir saugos politikos įgyvendinamiesiems dokumentams;

10.2. skiria saugos įgaliotinį, duomenų valdymo įgaliotinį, kibernetinio saugumo vadovą ir registro administratorių;

10.3. rengia registro saugos dokumentus ir teikia juos tvirtinti registro valdytojui;

10.4. teikia registro valdytojui pasiūlymus dėl registro plėtros, saugos ir funkcionalumo;

10.5. organizuoja plėtrą ir registro pakeitimų įdiegimą;

10.6. rūpinasi registro elektroninės informacijos saugumu, užtikrina tinkamą registro administravimą ir nepertraukiamą registro veiklą;

10.7. koordinuoja ir kontroliuoja Administracijos valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartis, kurie naudoja registrą paskirtoms funkcijoms vykdyti, bei registro paslaugos teikėjo (-ų) darbuotojų (toliau kartu – registro naudotojai) veiklą;

10.8. užtikrina registro elektroninės informacijos tvarkymo teisėtumą, saugumą ir registro saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams ir registro saugos dokumentams;

10.9. atlieka kitas registro valdytojo pavestas, registro saugos dokumentuose bei teisės aktuose, reglamentuojančiuose saugų elektroninės informacijos tvarkymą, priskirtas funkcijas.

11. Registro paslaugos teikėjo (-ų) vadovas (-ai) paskiria administratorių (-ius) (toliau – registro paslaugos teikėjo administratorius), jis nurodomas Administracijos ir registro paslaugų teikėjo (-ų) sudarytoje (-ose) sutartyje (-yse).

12. Saugos įgaliotinis atlieka šias funkcijas:

12.1. teikia pasiūlymus Administracijos vadovui dėl:

12.1.1. registro administratoriaus paskyrimo ir reikalavimų jam nustatymo;

12.1.2. registro informacinių technologijų saugos atitikties vertinimo atlikimo, remiantis Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – IT saugos atitikties vertinimo metodika);

12.1.3. registro saugos dokumentų priėmimo, keitimo ar panaikinimo;

12.2. užtikrina tinkamą registro saugos reikalavimų ir funkcijų vykdymą;

12.3. organizuoja registro rizikos įvertinimą, prireikus – neeilinį registro rizikos įvertinimą ir registro informacinių technologijų saugos atitikties vertinimą;

12.4. informuoja pagal kompetenciją Administracijos vadovą apie registro saugos problemas;

12.5. teikia registro administratoriui, registro paslaugos teikėjo administratoriui, registro naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;

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

12.7. bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų saugos incidentus, neteisėtas veikas, susijusias su elektroninės informacijos sauga, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės;

12.8. užtikrina registro saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams;

12.9. pasirašytinai supažindina registro administratorių, registro paslaugos teikėjo administratorių ir registro naudotojus su registro saugos dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, ir atsakomybe už šių dokumentų reikalavimų nesilaikymą;

12.10. periodiškai inicijuoja registro administratoriaus, registro paslaugos teikėjo administratoriaus ir registro naudotojų mokymus elektroninės informacijos saugos klausimais, įvairiais būdais informuoja juos apie elektroninės informacijos saugos problemas (teminiai seminarai, atmintinės priimtiems naujiems darbuotojams ir pan.);

12.11. atlieka kitas Administracijos vadovo pavestas užduotis, registro saugos dokumentuose ir kituose saugos reikalavimus nustatančiuose teisės aktuose jam priskirtas funkcijas.

13. Saugos įgaliotinis negali atlikti registro administratoriaus funkcijų.

14. Registro administratorius atlieka šias funkcijas:

14.1. atlieka registro naudotojams priskirtų funkcijų ir suteiktų teisių atitikties vertinimą, administruoja šias teises;

14.2. rengia ir tikrina registro komponentų sąranką, teikia saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę, saugos politikos pažeidimus, nustatytas registro pažeidžiamas vietas;

14.3. ne rečiau kaip kartą per metus ir (arba) atlikus registro pakeitimus tikrina (peržiūri) registro komponentų sąranką ir registro būsenos rodiklius;

14.4. pagal kompetenciją rengia ir teikia Administracijos vadovui ir saugos įgaliotiniui pasiūlymus dėl registro kūrimo, palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

14.5. pagal kompetenciją reaguoja į saugos incidentus, registruoja juos ir informuoja apie juos saugos įgaliotinį, teikia pasiūlymus dėl minėtų incidentų šalinimo, taip pat informuoja saugos įgaliotinį apie nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones;

14.6. nustato registro pažeidžiamas vietas, vykdo saugumo reikalavimų atitikties stebėseną;

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

14.8. vykdo saugos įgaliotinio nurodymus ir pavedimus, susijusius su registro saugos politikos įgyvendinimu;

14.9. registruoja ir deaktyvuoja registro naudotojus, nustato prieigos prie registro teises;

14.10. užtikrina įdiegtą registro sąveiką su kitomis informacinėmis sistemomis ir registrais;

14.11. pagal kompetenciją administruoja techninės ir programinės įrangos, infrastruktūros bei informacinių technologijų paslaugas;

14.12. dalyvauja atkuriant registro elektroninę informaciją iš elektroninės informacijos atsarginių kopijų;

14.13. atlieka kitas registro saugos dokumentuose registro administratoriui priskirtas funkcijas ir vykdo kitus Administracijos vadovo nurodymus ir pavedimus, susijusius su registro užtikrinimu.

15. Administracija turi paskirti valstybės tarnautoją ar darbuotoją, dirbantį pagal darbo sutartį, kontroliuojantį registro paslaugos teikėjo administratorių.

16. Registro paslaugos teikėjo administratorius atlieka šias funkcijas:

16.1. reaguoja į saugos incidentus, registruoja juos ir informuoja registro administratorių apie nustatytus saugos politikos pažeidimus, teikia pasiūlymus dėl minėtų incidentų šalinimo, informuoja registro administratorių apie nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones;

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

16.3. vykdo registro paslaugos teikėjo darbuotojų, naudojančių registrą sutartiniams įsipareigojimams vykdyti, registre atliekamų veiksmų kontrolę;

16.4. atlieka kitas Administracijos ir registro paslaugos teikėjo sutartyje numatytas funkcijas, registro saugos dokumentuose registro paslaugos teikėjo administratoriui priskirtas funkcijas.

17. Kibernetinio saugumo vadovas atlieka šias funkcijas:

17.1. koordinuoja kibernetinių incidentų tyrimą, bendradarbiauja su kompetentingomis institucijomis, tiriančiomis kibernetinius incidentus;

17.2. atlieka kitas registro saugos dokumentuose nurodytas ir kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, jam priskirtas funkcijas.

18. Saugos įgaliotinis ir kibernetinio saugumo vadovas gali būti tas pats asmuo.

19. Teisės aktų, kuriais vadovaujamasi tvarkant registro elektroninę informaciją ir užtikrinant jos saugumą, sąrašas:

19.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

19.2. Valstybės informacinių išteklių valdymo įstatymas;

19.3. Kibernetinio saugumo įstatymas;

19.4. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“;

19.5. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Kibernetinio saugumo reikalavimų aprašas);

19.6. Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2023 m. liepos 19 d. nutarimu Nr. 576 „Dėl Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašo patvirtinimo“;

19.7. IT saugos atitikties vertinimo metodika;

19.8. Valstybės informacinių išteklių svarbos vertinimo metodika, patvirtinta Lietuvos Respublikos ekonomikos ir inovacijų ministro 2023 m. liepos 19 d. įsakymu Nr. 4-418 „Dėl Valstybės informacinių išteklių svarbos vertinimo metodikos patvirtinimo“;

19.9. Lietuvos standartai LST ISO/IEC 27002 ir LST ISO/IEC 27001, Lietuvos ir tarptautiniai „Informacinės technologijos. Saugumo metodai“ grupės standartai, nustatantys saugų informacinės sistemos duomenų tvarkymą;

19.10. registro nuostatai;

19.11. Saugos nuostatai;

19.12. saugos politikos įgyvendinamieji dokumentai.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

20. Vadovaujantis Metodikos 8.5.3 papunkčiu, registre tvarkoma elektroninė informacija priskiriama vidutinės svarbos valstybės informaciniams ištekliams.

21. Saugos įgaliotinis, atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacinės technologijos. Saugumo metodai“ grupės standartus, kasmet organizuoja registro rizikos įvertinimą, jeigu teisės aktai nenustato kitaip. Prireikus saugos įgaliotinis gali organizuoti neeilinį registro rizikos įvertinimą. Neeilinis registro rizikos įvertinimas atliekamas pasikeitus registro struktūrai (esminiai registro funkciniai pakitimai ir programinės įrangos keitimas), įvykus dideliems Administracijos organizaciniams pokyčiams, atsiradus naujų informacinių technologijų saugos srities reikalavimų, po saugos incidento, kurio metu buvo sutrikdyta registro veikla, sugadinta ar prarasta registre tvarkoma elektroninė informacija.

22. Registro rizikos įvertinimas atliekamas pagal kokybinį rizikos vertinimo metodą. Kartu su pagrindiniu registro rizikos įvertinimu organizuojamas ir atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos registro kibernetiniam saugumui, vertinimas. Administracijos vadovo rašytiniu pavedimu registro rizikos įvertinimą gali atlikti pats saugos įgaliotinis. Rizikos įvertinimui atlikti sutartiniais pagrindais gali būti perkamos registro rizikos įvertinimo paslaugos iš trečiųjų asmenų.

23. Registro rizikos įvertinimo rezultatai pateikiami rizikos įvertinimo ataskaitoje ir ji pateikiama Administracijos vadovui. Registro rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos registro elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Registro rizikos įvertinimo ataskaitą rengia arba, jei įvertinimą atlieka tretieji asmenys, dalyvauja rengiant saugos įgaliotinis. Svarbiausi rizikos veiksniai yra šie:

23.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai

elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);

23.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis registro elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

23.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

24. Rizikos įvertinimo metu atliekamos veiklos:

24.1. registrą sudarančių informacinių išteklių inventorizacija;

24.2. įtakos registro veiklai vertinimas;

24.3. grėsmės ir pažeidimų analizė;

24.4. liekamosios rizikos vertinimas.

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

26. Kibernetinio saugumo atitikties reikalavimams vertinimo metu taip pat turi būti atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos informacinių sistemų kibernetiniam saugumui, vertinimas, kurio metu imituojamos kibernetinės atakos ir vykdomos kibernetinių incidentų imitavimo pratybos. Kibernetinių atakų imitavimo etapai:

26.1. Planavimas. Parengiamas pažeidžiamumų nustatymo planas, kuriame apibrėžiami kibernetinių atakų imitavimo tikslai ir darbų apimtis, pateikiamas darbų grafikas, aprašomi planuojamų imituoti kibernetinių atakų tipai (išorinės ir (ar) vidinės), kibernetinių atakų imitavimo būdai (juodosios dėžės (angl. *Black Box*), baltosios dėžės (angl. *White Box*) ir (ar) pilkosios dėžės (angl. *Grey Box*), galima neigiama įtaka veiklai, kibernetinių atakų imitavimo metodologija, programiniai ir (ar) techniniai įrankiai ir priemonės, naudojami pažeidžiamumams nustatyti, nurodomos už pažeidžiamumų nustatymo plano vykdymą atsakingų asmenų teisės ir pareigos.

26.2. Žvalgyba (angl. *Reconnaissance*) ir aptikimas (angl. *Discovery*). Surenkama informacija apie perimetrą, tinklo mazgus, tinklo mazguose veikiančių tarnybinių stočių ir kitų tinklo įrenginių operacines sistemas ir programinę įrangą, paslaugas (angl. *Services*), pažeidžiamumą, konfigūracijas ir kitą sėkmingai kibernetinei atakai įvykdyti reikalingą informaciją.

26.3. Kibernetinių atakų imitavimas. Atliekami pažeidžiamumų nustatymo plane numatyti testai.

26.4. Ataskaitos parengimas. Kibernetinių atakų imitavimo rezultatai turi būti pateikti kibernetinio saugumo atitikties reikalavimams vertinimo ataskaitoje. Pažeidžiamumų nustatymo plane numatyti testų rezultatai turi būti detalizuojami ataskaitoje ir lyginami su planuotais. Kiekvienas aptiktas pažeidžiamumas turi būti detalizuojamas ir pateikiamos rekomendacijos jam pašalinti. Kibernetinių atakų imitavimo rezultatai turi būti pagrįsti patikimais įrodymais ir rizikos įvertinimu. Jeigu nustatoma incidentų valdymo ir šalinimo, taip pat organizacijos nepertraukiamos veiklos užtikrinimo trūkumų, turi būti tobulinami veiklos tęstinumo planai.

27. Atsižvelgiant į kibernetinio saugumo atitikties reikalavimams vertinimo ataskaitą, rengiamas nustatytų trūkumų šalinimo planas, kuriame, atsižvelgiant į kibernetinių atakų imitavimo metu nustatytus trūkumus, registro valdytojo vadovui teikiami pasiūlymai dėl kibernetinį saugumą reglamentuojančių teisės aktų ar kitų registro valdytojo vadovo patvirtintų dokumentų pakeitimo, kibernetinio saugumo būklės gerinimo ir papildomų kibernetinio saugumo priemonių įsigijimo. Nustatytų trūkumų šalinimo planą tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato registro valdytojo vadovas.

28. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas, kibernetinio saugumo atitikties reikalavimams vertinimo ataskaitos ir nustatytų

trūkumų šalinimo plano kopijas registro valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai (toliau – ARSIS) Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“ (toliau – Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatai) nustatyta tvarka.

29. Siekdamas užtikrinti Saugos nuostatų ir saugos politikos įgyvendinamųjų dokumentų nuostatų įgyvendinimo kontrolę, saugos įgaliotinis ne rečiau kaip kartą per metus, jeigu teisės aktai nenustato kitaip, organizuoja informacinių technologijų saugos atitikties vertinimą pagal IT saugos atitikties vertinimo metodikos reikalavimus.

30. Atliekant registro informacinių technologijų saugos atitikties vertinimą:

30.1. įvertinama esamos registro elektroninės informacijos saugos situacijos atitiktis registro saugos dokumentams ir kitiems elektroninės informacijos saugą reglamentuojantiems teisės aktams;

30.2. inventorizuojama registro techninė ir programinė įranga;

30.3. peržiūrima ir įvertinama registro administratoriui, registro paslaugos teikėjo administratoriui, registro naudotojams suteiktų teisių atitiktis jų atliekamoms funkcijoms;

30.4. duomenų saugos požiūriu patikrinama registro techninė ir programinė įranga: visos tarnybinės stotys ir ne mažiau kaip 10 proc. atsitiktinai parinktų registro naudotojų kompiuterinių darbo vietų (toliau – KDV);

30.5. įvertinamas pasirengimas užtikrinti registro veiklos tęstinumą įvykus saugos incidentui.

31. Atlikus registro informacinių technologijų saugos atitikties vertinimą, parengiama informacinių technologijų saugos atitikties vertinimo ataskaita ir pateikiama Administracijos vadovui, taip pat parengiamas pastebėtų trūkumų šalinimo planas. Registro valdytojo vadovas patvirtina šį planą, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminus.

32. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas registro valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti ARSIS Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

33. Prireikus saugos įgaliotinis gali organizuoti neeilinį registro informacinių technologijų saugos atitikties vertinimą.

34. Neeilinis registro informacinių technologijų saugos atitikties vertinimas atliekamas:

34.1. įvykus registro techninės ar programinės įrangos pokyčiams, kurie gali turėti įtakos registro veikimui;

34.2. paaiškėjus naujoms tendencijoms informacinių technologijų saugos srityje, dėl kurių kiltų grėsmė registro techninei, programinei įrangai ar registro tvarkomai elektroninei informacijai;

34.3. po saugos incidento, kurio metu buvo sutrikdyta registro veikla, sugadinta ar prarasta registro elektroninė informacija.

35. Techninės, programinės ir organizacinės registro elektroninės informacijos saugos priemonės pasirenkamos atsižvelgiant į registro valdytojo ir Administracijos turimus išteklius, vadovaujantis šiais priemonių parinkimo principais:

35.1. Liekamoji rizika turi būti sumažinta iki priimtino lygio.

35.2. Informacijos saugos priemonės diegimo kaina turi būti adekvati saugomos informacijos vertei.

35.3. Esant galimybei, turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

36. 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 eksploatuojamo registro.

37. Registro pokyčius gali inicijuoti saugos įgaliotinis ar registro administratorius, o įgyvendina registro administratorius.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

38. Nustatomi šie registro naudojamos programinės įrangos reikalavimai:

38.1. Registro naudojama programinė įranga turi atitikti programinės įrangos saugos gerąją praktiką, kuriant programinę įrangą taikomą saugos gerąją praktiką, programinės įrangos kūrimo struktūras, standartus.

38.2. Specifiniai saugos reikalavimai turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose.

38.3. Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos.

38.4. Programinės įrangos kūrimo, testavimo ir verifikacijos etapai turi vykti atsižvelgiant į pagrindinius saugos reikalavimus.

38.5. Prieš pradedant naudoti programinę įrangą, turi būti atliktas šios programinės įrangos pažeidžiamumo, pritaikomumo ir infrastruktūros atsparumo skverbimuisi įvertinimas. Programinė įranga negali būti patvirtinta, kol nėra pasiektas reikiamas saugumo lygis.

38.6. Turi būti atliekami periodiški infrastruktūros atsparumo skverbimuisi testavimai.

39. Programinės įrangos, skirtos registrui ir KDV apsaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos:

39.1. Registre turi būti naudojama antivirusinė programinė įranga, skirta registrui apsaugoti nuo kenksmingos programinės įrangos.

39.2. Antivirusinė programinė įranga turi būti atnaujinama automatiškai ne rečiau kaip kartą per parą.

39.3. Registro naudotojų kompiuteriuose naudojama įranga, skirta KDV apsaugoti nuo kenksmingos programinės įrangos, turi apsaugoti ir elektroninio pašto programinę įrangą nuo nepageidaujamo pašto ar kenksmingų programų patekimo į KDV.

39.4. Atsiradus požymių, kad KDV yra kenksmingų programų, turi būti patikrinami visi KDV standieji diskai, naudojama programinė įranga, skirta registrui ir KDV apsaugoti nuo kenksmingos programinės įrangos.

39.5. KDV esančios programinės įrangos, skirtos registrui ir KDV apsaugoti nuo kenksmingos programinės įrangos, nustatymai turi būti parinkti pagal rekomenduojamus tokios programinės įrangos gamintojų reikalavimus arba pagal vidinio kompiuterių tinklo administratoriaus rekomendacijas.

39.6. Programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

39.7. Apsaugos sistema privalo automatiškai informuoti registro paslaugos teikėjo administratorių apie KDV ir tarnybines stotis, kuriose apsaugos sistema netinkamai funkcionuoja, yra išjungta arba neatsinaujino per 24 valandas.

39.8. Registro operacinės sistemos ir naudojami programinės įrangos gamintojų rekomenduojami atnaujinimai turi būti įdiegiami nedelsiant, nesutrikdant registro paslaugų teikimo ir suderinus atnaujinimų darbus su registro administratoriumi.

39.9. Registro naudotojų kompiuterių apsaugos priemonės yra valdomos (ugniasienių įjungimas ir konfigūravimas, antivirusinių programų ir operacinių sistemų atnaujinimas) centralizuotai.

40. Metodai ir priemonės, kurie taikomi užtikrinant prieigą prie registro:

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

40.2. Registro priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą administratoriaus klasifikatorių, kuriuo naudojantis nebūtų galima atlikti registro naudotojo funkcijų.

40.3. Registro naudotojas turi būti registre unikaliai identifikuojamas – registro naudotojas turi patvirtinti savo tapatybę slaptažodžiu, registro naudotojui suteiktas pirminis slaptažodis turi būti pakeistas pirmo prisijungimo metu. Slaptažodžiai sudaromi, keičiami ir jų galiojimo trukmė nustatoma vadovaujantis Lietuvos Respublikos jūrininkų registro naudotojų administravimo taisyklėmis.

40.4. Prieigą prie registro suteikia, apriboja ir panaikina registro administratorius.

40.5. Teisė dirbti su konkrečia elektronine informacija suteikiama konkrečiam registro naudotojui.

40.6. Registro naudotojui teisė dirbti su konkrečia elektronine informacija turi būti ribojama ar sustabdoma, kai registro naudotojas neprisijungė ilgiau kaip 2 mėnesius, vykdomas registro naudotojo veiklos tyrimas ir pan. Pasibaigus valstybės tarnybos ar darbo santykiams, registro naudotojo teisė naudotis registru turi būti panaikinta.

40.7. Baigus darbą ar pasitraukiant iš darbo vietos, turi būti imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo registro, įjungiama ekrano užsklanda su slaptažodžiu, dokumentai padedami į pašaliniams asmenims neprieinamą vietą.

40.8. Registro naudotojui 15 min. neatliekant jokių veiksmų informacinėje sistemoje, registras turi užsirakinti, kad toliau naudotis registru būtų galima tik pakartojus tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus.

40.9. Prisijungimo prie kompiuterių tinklo laikas ir trukmė nėra ribojami, registras pasiekiamas visą parą.

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

41.1. Registre turi būti naudojama tik legali programinė įranga.

41.2. Draudžiama diegti ir naudoti bet kokią programinę įrangą, keisti sistemos, kompiuterio ar programinės įrangos sistemų nustatymus. Programinę įrangą, reikalingą registro naudotojo funkcijoms atlikti, KDV diegia, atnaujina, kontroliuoja ir prižiūri atsakingi Administracijos valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis, ar registro paslaugų teikėjo darbuotojai. Kiti asmenys (registro paslaugų teikėjų specialistai) gali diegti programinę įrangą tik suderinus su registro administratoriumi.

41.3. Diegti ir naudoti programinę įrangą, nesusijusią su registro valdytojo ar Administracijos veikla ar registro naudotojo atliekamomis funkcijomis (žaidimų, bylų siuntimo, internetinių pokalbių programas ir kt.), draudžiama.

41.4. Tarnybinėse stotyse ir registro naudotojų KDV privalo būti naudojama programinė įranga, kuri apsaugo nuo kenksmingos programinės įrangos ir kuri turi būti atnaujinama ne rečiau kaip kartą per parą laikantis gamintojo reikalavimų.

41.5. KDV, programinė įranga, jos sertifikatai ir licencijos kasmet turi būti inventorizuojami.

41.6. Naudojama programinė įranga, leidžianti atlikti registre naudojamų kompiuterių tinklų stebėseną ir užtikrinanti šių tinklų saugos prevencines priemones.

41.7. Programinė įranga yra nuolat atnaujinama laikantis gamintojo reikalavimų.

42. Leistinos kompiuterių (ypač nešiojamųjų) naudojimo ribos ir metodai, kuriais leidžiama užtikrinti saugų registro duomenų teikimą ir (ar) gavimą:

42.1. Stacionariuosiuose ir nešiojamuosiuose kompiuteriuose registro įjungimo metu turi būti identifikuojamas registro naudotojas.

42.2. Stacionarieji ir nešiojamieji registro naudotojų kompiuteriai privalo būti naudojami tik su tiesioginių pareigų atlikimu susijusiai veiklai. Iš kompiuterių, kurie perduodami remontui ar techninei priežiūrai, turi būti pašalinta visa neskelbtina registro elektroninė informacija.

42.3. Registro naudotojų nešiojamiesiems kompiuteriams ne Administracijos ar registro paslaugos teikėjo patalpose privaloma naudoti papildomas saugos priemones, kuriomis registro duomenys perduodami saugiu šifruotu virtualiu privačiu tinklu (angl. V*irtual Private Network*, toliau – VPN).

42.4. Registro naudotojai, darbinėms funkcijoms atlikti naudojantys nešiojamuosius kompiuterius, išnešdami juos iš Administracijos patalpų, norėdami registro elektroninę informaciją perduoti kompiuterių tinklais ne savo darbo vietoje, turi naudoti vieną iš išvardintų metodų: duomenų šifravimą, papildomą naudotojo tapatybės patvirtinimą, rakinimo įrenginį. Nešiojamojo kompiuterio pagrindinės įvesties ir išvesties sistema (BIOS) turi būti apsaugota slaptažodžiu ir nurodytas standusis diskas kaip pirminis paleidimo įrenginys. Iš išorės prie registro duomenų bazės prisijungimas ribojamas. Nešiojamuosiuose kompiuteriuose ar išorinėse kompiuterinėse laikmenose esantys duomenys turi būti šifruojami. Registro naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo.

43. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kt.) pagrindinės naudojimo nuostatos:

43.1. Techninis nuotolinio prisijungimo sprendimas turi užtikrinti ne žemesnį nei vidiniam prisijungimui naudojamą saugumo lygį, t. y. turi būti naudojamos Saugos nuostatuose minimos priemonės, duomenų perdavimas saugiu šifruotu VPN arba naudojant saugų duomenų perdavimo protokolą HTTPS (angl. *Hypertext Transfer Protocol Secure*).

43.2. Registro naudotojams, kuriems atliekant tiesiogines pareigas būtina prisijungti iš nutolusios darbo vietos, gali būti suteikiama nuotolinio prisijungimo prie registro galimybė.

43.3. Kompiuterinis tinklas, prie kurio prijungtos registro tarnybinės stotys ir registro naudotojų kompiuteriai, nuo viešojo interneto turi būti atskirtas ugniasienėmis ir įsilaužimų aptikimo ir prevencijos įranga, už kurios administravimą ir priežiūrą atsakingas registro paslaugos teikėjo administratorius.

43.4. Visas duomenų srautas į internetą ir iš jo yra filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos.

43.5. Naudojamos turinio filtravimo sistemos.

43.6. Naudojama programinė įranga, leidžianti atlikti registre naudojamų kompiuterių tinklų monitoringą ir užtikrinanti šių tinklų saugos prevencines priemones.

43.7. Registro tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių informacinės sistemos naudotojų kompiuterinę įrangą nuo kenksmingo kodo (naudojama antivirusinė programa).

43.8. Registro programinė įranga turi būti apsaugota nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS)*, dedikuoto atkirtimo nuo paslaugos (angl. *DDOS*) ir kitų. Pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project (OWASP*) interneto svetainėje www.owasp.org.

43.9. Už saugų registro kompiuterių tinklų veikimą pagal kompetenciją atsako Administracijos kompiuterių tinklų administratorius.

44. Užtikrinant saugų elektroninės informacijos teikimą kitoms valstybės institucijoms ir (ar) gavimą iš jų, naudojamas šifruotas VPN arba Saugus valstybinis duomenų perdavimo tinklas (toliau – SVDPT). Elektronine informacija keičiamasi per saugų duomenų perdavimo protokolą HTTPS žiniatinklio paslaugų metodu (XML formatu) arba duomenų bazių užklausomis. Duomenys teikiami ir (ar) gaunami automatizuotomis priemonėmis tik pagal duomenų teikimo sutartyje nustatytas specifikacijas, duomenų perdavimo sąlygas ir tvarką.

45. Metodai, kuriais gali būti užtikrinamas saugus registro elektroninės informacijos teikimas ir (ar) gavimas:

45.1. Iš registro duomenų teikėjų elektroninė informacija gaunama pagal duomenų teikimo sutartyse numatytas elektroninės informacijos perdavimo technologijas, jų šifravimo mechanizmus, specifikacijas ir kitas sąlygas.

45.2. Duomenų gavėjų prieigą prie registro kontroliuoja kompiuterių tinklo užkarda.

45.3. Už registro elektroninės informacijos teikimo ir gavimo duomenų teikimo sutartyse nurodomų saugos reikalavimų nustatymą, suformulavimą ir įgyvendinimo organizavimą atsakingas saugos įgaliotinis.

45.4. Registro elektroninei informacijai perduoti naudojamas SVDPT arba kitas šifruotas perdavimo kanalas, užtikrinantis saugų elektroninės informacijos perdavimą.

46. Pagrindiniai atsarginių registro elektroninės informacijos kopijų (toliau – atsarginės kopijos) darymo ir atkūrimo reikalavimai:

46.1. Registro veiklos tęstinumui užtikrinti registro duomenys yra periodiškai, bet ne rečiau kaip kas 24 valandas kopijuojami į rezervinių kopijų laikmenas ir laikmenos saugomos taip, kad, įvykus saugos incidentui, visiškas registro funkcionalumas ir veikla būtų atkurti per 12 valandų.

46.2. Atsarginėms kopijoms kurti turi būti naudojama speciali programinė įranga.

46.3. Privalo būti visos saugomos elektroninės informacijos rezervinio kopijavimo funkcija.

46.4. Registro administratorius privalo turėti galimybę inicijuoti elektroninės informacijos atkūrimo iš rezervinės kopijos procedūrą pasirinktinai iš turimų rezervinių kopijų sąrašo. Atkūrus elektroninę informaciją privalo būti užtikrintas ir išlaikytas elektroninės informacijos vientisumas ir integralumas.

46.5. Registro elektroninė informacija registro naudotojams turi būti prieinama ne mažiau kaip 96 procentus sistemos veikimo laiko visą parą.

46.6. Elektroninė informacija atsarginėse kopijose turi būti šifruota (šifravimo raktai turi būti saugomi atskirai nuo atsarginių kopijų).

46.7. Atsarginės kopijos yra daromos ir saugomos taip, kad jos nebūtų prieinamos tretiesiems asmenims, kurie neturi teisės su jomis dirbti.

46.8. Atsarginės kopijos turi būti laikomos atskirai nuo tarnybinių stočių. Už atsarginių kopijų darymą, atkūrimą ir atkūrimo iš atsarginių kopijų testavimą yra atsakinga Administracija.

46.9. Atkūrimo iš atsarginių kopijų funkcija privalo būti išbandoma ne rečiau kaip kartą per pusmetį. Testavimo eiga ir rezultatai įforminami atsarginių kopijų darymo žurnale. Duomenų atkūrimo bandymą organizuoja saugos įgaliotinis.

47. Nustatomi duomenų naikinimo ir šalinimo reikalavimai:

47.1. Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinta visa joje esanti elektroninė informacija, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Jeigu to padaryti neįmanoma (pvz., DVD laikmenos), duomenų laikmenos turi būti fiziškai sunaikinamos be galimybės atkurti duomenis.

47.2. Prieš šalinant laikmenas, turi būti atlikti visų šalinamų laikmenų daugybiniai programinės įrangos perrašymai.

48. Jeigu saugiems duomenų naikinimo ir šalinimo duomenų laikmenose darbams atlikti yra pasitelkiamos trečiųjų asmenų paslaugos, turi būti sudaryta atitinkama paslaugų sutartis.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

49. Tvarkyti registro duomenis gali asmenys, susipažinę su Reglamentu (ES) 2016/679, registro nuostatais, registro saugos dokumentais, registrų ir informacinių sistemų saugos politiką reglamentuojančiais teisės aktais.

50. Registro naudotojai turi būti įgiję darbo kompiuteriu įgūdžių, mokėti tvarkyti registro elektroninę informaciją registro nuostatuose nurodyta tvarka, išmanyti registrų ir informacinių sistemų saugos politiką reglamentuojančius teisės aktus. Tvarkyti registro elektroninę informaciją gali tik registro naudotojai, pasirašę pasižadėjimą saugoti asmens duomenų paslaptį. Ši pareiga galioja perėjus dirbti į kitas pareigas arba pasibaigus valstybės tarnybos, darbo, sutartiniams ar kitiems santykiams.

51. Saugos įgaliotinis privalo išmanyti šiuolaikinių informacinių technologijų panaudojimo ypatumus, žinoti elektroninės informacijos saugos užtikrinimo principus bei metodus, rizikų valdymą, savo darbe vadovautis Reglamentu (ES) 2016/679, Aprašu, IT saugos atitikties vertinimo metodika, registro saugos dokumentais, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais elektroninės informacijos saugą, kibernetinę saugą, taip pat būti susipažinęs su esminiais registro elektroninės informacijos saugos reikalavimais. Saugos įgaliotinis privalo sugebėti prižiūrėti, kaip įgyvendinama saugos politika. Saugos įgaliotinis kiekvienais metais privalo tobulinti kvalifikaciją elektroninės informacijos saugos srityje.

52. Kibernetinio saugumo vadovas privalo išmanyti kibernetinio saugumo užtikrinimo principus, kiekvienais metais tobulinti kvalifikaciją kibernetinio saugumo srityje ir savo darbe vadovautis registro saugos dokumentais, Kibernetinio saugumo reikalavimų aprašu, Lietuvos Respublikos ir Europos Sąjungos teisės aktais, standartais, reglamentuojančiais kibernetinį saugumą.

53. Saugos įgaliotiniu ir kibernetinio saugumo vadovu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą galiojančią 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 nuobaudos paskyrimo praėję mažiau kaip vieni metai.

54. Registro administratorius ar registro paslaugos teikėjo administratorius privalo išmanyti darbą su kompiuterių tinklais ir mokėti užtikrinti jų saugumą, būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais, žinoti tarnybinių stočių veikimo principus, gebėti užtikrinti techninės ir programinės įrangos nepertraukiamą funkcionavimą bei saugą, stebėti techninės ir programinės įrangos veikimą, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, sutrikimų bei saugos incidentų diagnostiką ir šalinimą.

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

56. Registro naudotojų, registro administratoriaus ir registro paslaugos teikėjo administratoriaus mokymai organizuojami taip, kaip numatyta Saugos nuostatų 12.10 papunktyje, ne rečiau kaip kartą per metus. Mokymus organizuoja ir jų efektyvumą vertina saugos įgaliotinis.

V SKYRIUS
REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

57. Registro naudotojų, registro administratoriaus ir registro paslaugos teikėjo administratoriaus supažindinimą su registro saugos dokumentais ar kitais elektroninės informacijos saugą reglamentuojančiais teisės aktais ir atsakomybe, kylančia dėl jų pažeidimo,

atlieka saugos įgaliotinis pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodymą.

58. Registro administratorių ir registro paslaugos teikėjo administratorių su registro saugos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodymą, supažindina saugos įgaliotinis per 10 darbo dienų nuo registro administratoriaus ar registro paslaugos teikėjo administratoriaus paskyrimo.

59. Registro naudotojus su registro saugos dokumentais ir teisės aktais, reglamentuojančiais registro elektroninės informacijos saugą, saugos įgaliotinis pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodymą, supažindina prieš sukuriant registro naudotojo prisijungimo duomenis.

60. Pakartotinai su registro saugos dokumentais ir teisės aktais, reglamentuojančiais registro elektroninės informacijos saugą, saugos įgaliotinis pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodymą, supažindina registro naudotojus, registro administratorių ir registro paslaugos teikėjo administratorių kitą darbo dieną po registro saugos dokumentų ir teisės aktų, reglamentuojančių registro elektroninės informacijos saugą, priėmimo (išdėstymo nauja redakcija), pakeitimo ar pripažinimo netekusiais galios.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

61. Saugos įgaliotinis organizuoja registro saugos dokumentų persvarstymą ne rečiau kaip kartą per metus. Registro saugos dokumentai turi būti persvarstomi atlikus rizikos analizę ar informacinių technologijų saugos atitikties vertinimą, pasikeitus saugos politiką reglamentuojantiems teisės aktams, įvykus esminiams organizaciniams, technologiniams ar kitiems registro pokyčiams, po įvykusio kibernetinio incidento.

62. Saugos įgaliotinis, kibernetinio saugumo vadovas, registro administratorius, registro paslaugos teikėjo administratorius, registro naudotojai ir kiti subjektai, kuriems taikomi Saugos nuostatų reikalavimai, pažeidę registro saugos dokumentų ir kitų teisės aktų, reglamentuojančių saugų elektroninės informacijos tvarkymą, reikalavimus, atsako Lietuvos Respublikos teisės aktų, reguliuojančių valstybės registrų ir informacinių sistemų saugą, nustatyta tvarka.

_____

PATVIRTINTA
Lietuvos Respublikos susisiekimo ministro
2016 m. vasario 9 d. įsakymu Nr. 3-48(1.5 E)
(Lietuvos Respublikos susisiekimo ministro
2024 m. balandžio 19 d. įsakymo Nr. 3-138
redakcija)

LIETUVOS RESPUBLIKOS JŪRŲ LAIVŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos jūrų laivų registro duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Lietuvos Respublikos jūrų laivų registro (toliau – registras) elektroninės informacijos saugos politiką ir kibernetinio saugumo politiką (toliau – saugos politika), kurių tikslas – nustatyti ir įgyvendinti organizacines, administracines, technines ir kitas priemones, suteikiančias galimybę saugiai tvarkyti registro duomenis ir užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo netyčinio ar neteisėto sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jos.

2. Saugos nuostatuose vartojamos sąvokos suprantamos taip, kaip jos yra apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, 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 ir Saugos dokumentų turinio gairių aprašo patvirtinimo“ (toliau – Aprašas).

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

3.1. Lietuvos Respublikos jūrų laivų registro saugaus elektroninės informacijos tvarkymo taisyklės;

3.2. Lietuvos Respublikos jūrų laivų registro naudotojų administravimo taisyklės;

3.3. Lietuvos Respublikos jūrų laivų registro veiklos tęstinumo valdymo planas.

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

5. Registro elektroninės informacijos saugos ir kibernetinio saugumo (toliau – registro elektroninės informacijos sauga) užtikrinimo tikslai:

5.1. sudaryti sąlygas saugiai automatizuotomis priemonėmis tvarkyti registro elektroninę informaciją;

5.2. užtikrinti registro elektroninės informacijos patikimumą, konfidencialumą, prieinamumą, vientisumą ir tinkamą techninės, programinės ir ryšių įrangos funkcionavimą;

5.3. vykdyti elektroninės informacijos saugos ir kibernetinių incidentų (toliau – saugos incidentai), asmens duomenų saugumo pažeidimų prevenciją, reaguoti į saugos incidentus, asmens duomenų saugumo pažeidimus ir juos operatyviai suvaldyti.

6. Registro elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

6.1. registro elektroninei informacijai tvarkyti naudojamos techninės ir programinės įrangos kontrolė;

6.2. registro elektroninės informacijos tvarkymo kontrolė;

6.3. saugaus darbo su registro elektronine informacija kontrolė;

6.4. fizinė registro elektroninės informacijos tvarkymo priemonių (tarnybinių stočių, informacijos perdavimo įrangos, programinės įrangos) ir patalpų apsauga;

6.5. registro veiklos tęstinumas.

7. Registro valdytoja ir asmens duomenų valdytoja yra Lietuvos Respublikos susisiekimo ministerija, esanti adresu Gedimino pr. 17, 01103 Vilnius (toliau – registro valdytojas). Registro tvarkytoja ir asmens duomenų tvarkytoja yra Lietuvos transporto saugos administracija, esanti adresu Švitrigailos g. 42, 03209 Vilnius (toliau – Administracija).

8. Saugos nuostatais privalo vadovautis:

8.1. Administracijos valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis, registro saugos įgaliotinis (toliau – saugos įgaliotinis), registro administratorius, asmuo ar padalinys, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą (toliau – kibernetinio saugumo vadovas), registro duomenų valdymo įgaliotinis (toliau – duomenų valdymo įgaliotinis);

8.2. Administracijos Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka išrinkto juridinio asmens ar asmenų (asmenų grupės), kuriems Valstybės informacinių išteklių valdymo įstatymo 39 straipsnyje nustatytomis sąlygomis ir tvarka perduotos registro ir (ar) jo infrastruktūros priežiūros funkcijos (toliau – registro paslaugos teikėjas (-ai)), darbuotojai;

8.3. kiti subjektai, kuriems taikomi Saugos nuostatų reikalavimai.

9. Registro valdytojas atlieka šias funkcijas:

9.1. formuoja registro saugos politiką ir organizuoja jos įgyvendinimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą;

9.2. tvirtina registro saugos dokumentus, prižiūri ir kontroliuoja, kad registras būtų tvarkomas vadovaujantis šiais dokumentais, registro nuostatais ir kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą;

9.3. nagrinėja Administracijos pasiūlymus dėl registro elektroninės informacijos saugos tobulinimo ir priima dėl jų sprendimus;

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

9.5. atsižvelgdamas į kibernetinio saugumo atitikties reikalavimams vertinimo ataskaitą, prireikus tvirtina nustatytų trūkumų šalinimo planą;

9.6. priima sprendimą atlikti registro informacinių technologijų saugos atitikties vertinimą;

9.7. prireikus tvirtina registro informacinių technologijų saugos atitikties vertinimo metu pastebėtų trūkumų šalinimo planą;

9.8. įgyvendina registro pokyčius ir plėtrą;

9.9. pagal kompetenciją užtikrina registro elektroninės informacijos saugos priemones;

9.10. paveda Administracijai paskirti saugos įgaliotinį, duomenų valdymo įgaliotinį, registro administratorių, kibernetinio saugumo vadovą;

9.11. vykdo kitas registro saugos dokumentų ir kitų teisės aktų, reglamentuojančių saugų elektroninės informacijos tvarkymą, nustatytas funkcijas.

10. Administracija atlieka šias funkcijas:

10.1. įgyvendina reikiamas administracines, technines ir organizacines saugos priemones, užtikrina registro saugos reikalavimų atitiktį Saugos nuostatams ir saugos politikos įgyvendinamiesiems dokumentams;

10.2. skiria saugos įgaliotinį, duomenų valdymo įgaliotinį, kibernetinio saugumo vadovą ir registro administratorių;

10.3. rengia registro saugos dokumentus ir teikia juos tvirtinti registro valdytojui;

10.4. teikia registro valdytojui pasiūlymus dėl registro plėtros, saugos ir funkcionalumo;

10.5. organizuoja plėtrą ir registro pakeitimų įdiegimą;

10.6. rūpinasi registro elektroninės informacijos saugumu, užtikrina tinkamą registro administravimą ir nepertraukiamą registro veiklą;

10.7. koordinuoja ir kontroliuoja Administracijos valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartis, kurie naudoja registrą paskirtoms funkcijoms vykdyti, bei registro paslaugos teikėjo (-ų) darbuotojų (toliau kartu – registro naudotojai) veiklą;

10.8. užtikrina registro elektroninės informacijos tvarkymo teisėtumą, saugumą ir registro saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams ir registro saugos dokumentams;

10.9. atlieka kitas registro valdytojo pavestas, registro saugos dokumentuose bei teisės aktuose, reglamentuojančiuose saugų elektroninės informacijos tvarkymą, priskirtas funkcijas.

11. Registro paslaugos teikėjo (-ų) vadovas (-ai) paskiria administratorių (-ius) (toliau – registro paslaugos teikėjo administratorius), jis nurodomas Administracijos ir registro paslaugų teikėjo (-ų) sudarytoje (-ose) sutartyje (-yse).

12. Saugos įgaliotinis atlieka šias funkcijas:

12.1. teikia pasiūlymus Administracijos vadovui dėl:

12.1.1. registro administratoriaus paskyrimo ir reikalavimų jam nustatymo;

12.1.2. registro informacinių technologijų saugos atitikties vertinimo atlikimo, remiantis Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – IT saugos atitikties vertinimo metodika);

12.1.3. registro saugos dokumentų priėmimo, keitimo ar panaikinimo;

12.2. užtikrina tinkamą registro saugos reikalavimų ir funkcijų vykdymą;

12.3. organizuoja registro rizikos įvertinimą, prireikus – neeilinį registro rizikos įvertinimą ir registro informacinių technologijų saugos atitikties vertinimą;

12.4. informuoja pagal kompetenciją Administracijos vadovą apie registro saugos problemas;

12.5. teikia registro administratoriui, registro paslaugos teikėjo administratoriui, registro naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;

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

12.7. bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų saugos incidentus, neteisėtas veikas, susijusias su elektroninės informacijos sauga, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės;

12.8. užtikrina registro saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams;

12.9. pasirašytinai supažindina registro administratorių, registro paslaugos teikėjo administratorių ir registro naudotojus su registro saugos dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, ir atsakomybe už šių dokumentų reikalavimų nesilaikymą;

12.10. periodiškai inicijuoja registro administratoriaus, registro paslaugos teikėjo administratoriaus ir registro naudotojų mokymus elektroninės informacijos saugos klausimais, įvairiais būdais informuoja juos apie elektroninės informacijos saugos problemas (teminiai seminarai, atmintinės priimtiems naujiems darbuotojams ir pan.);

12.11. atlieka kitas Administracijos vadovo pavestas užduotis, registro saugos dokumentuose ir kituose saugos reikalavimus nustatančiuose teisės aktuose jam priskirtas funkcijas.

13. Saugos įgaliotinis negali atlikti registro administratoriaus funkcijų.

14. Registro administratorius atlieka šias funkcijas:

14.1. atlieka registro naudotojams priskirtų funkcijų ir suteiktų teisių atitikties vertinimą, administruoja šias teises;

14.2. rengia ir tikrina registro komponentų sąranką, teikia saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę, saugos politikos pažeidimus, nustatytas registro pažeidžiamas vietas;

14.3. ne rečiau kaip kartą per metus ir (arba) atlikus registro pakeitimus tikrina (peržiūri) registro komponentų sąranką ir registro būsenos rodiklius;

14.4. pagal kompetenciją rengia ir teikia Administracijos vadovui ir saugos įgaliotiniui pasiūlymus dėl registro kūrimo, palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

14.5. pagal kompetenciją reaguoja į saugos incidentus, registruoja juos ir informuoja apie juos saugos įgaliotinį, teikia pasiūlymus dėl minėtų incidentų šalinimo, taip pat informuoja saugos įgaliotinį apie nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones;

14.6. nustato registro pažeidžiamas vietas, vykdo saugumo reikalavimų atitikties stebėseną;

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

14.8. vykdo saugos įgaliotinio nurodymus ir pavedimus, susijusius su registro saugos politikos įgyvendinimu;

14.9. registruoja ir deaktyvuoja registro naudotojus, nustato prieigos prie registro teises;

14.10. užtikrina įdiegtą registro sąveiką su kitomis informacinėmis sistemomis ir registrais;

14.11. pagal kompetenciją administruoja techninės ir programinės įrangos, infrastruktūros bei informacinių technologijų paslaugas;

14.12. dalyvauja atkuriant registro elektroninę informaciją iš elektroninės informacijos atsarginių kopijų;

14.13. atlieka kitas registro saugos dokumentuose registro administratoriui priskirtas funkcijas ir vykdo kitus Administracijos vadovo nurodymus ir pavedimus, susijusius su registro užtikrinimu.

15. Administracija turi paskirti valstybės tarnautoją ar darbuotoją, dirbantį pagal darbo sutartį, kontroliuojantį registro paslaugos teikėjo administratorių.

16. Registro paslaugos teikėjo administratorius atlieka šias funkcijas:

16.1. reaguoja į saugos incidentus, registruoja juos ir informuoja registro administratorių apie nustatytus saugos politikos pažeidimus, teikia pasiūlymus dėl minėtų incidentų šalinimo, informuoja registro administratorių apie nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones;

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

16.3. vykdo registro paslaugos teikėjo darbuotojų, naudojančių registrą sutartiniams įsipareigojimams vykdyti, registre atliekamų veiksmų kontrolę;

16.4. atlieka kitas Administracijos ir registro paslaugos teikėjo sutartyje numatytas funkcijas, registro saugos dokumentuose registro paslaugos teikėjo administratoriui priskirtas funkcijas.

17. Kibernetinio saugumo vadovas atlieka šias funkcijas:

17.1. koordinuoja kibernetinių incidentų tyrimą, bendradarbiauja su kompetentingomis institucijomis, tiriančiomis kibernetinius incidentus;

17.2. atlieka kitas registro saugos dokumentuose nurodytas ir kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, jam priskirtas funkcijas.

18. Saugos įgaliotinis ir kibernetinio saugumo vadovas gali būti tas pats asmuo.

19. Teisės aktų, kuriais vadovaujamasi tvarkant registro elektroninę informaciją ir užtikrinant jos saugumą, sąrašas:

19.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

19.2. Valstybės informacinių išteklių valdymo įstatymas;

19.3. Kibernetinio saugumo įstatymas;

19.4. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“;

19.5. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Kibernetinio saugumo reikalavimų aprašas);

19.6. Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2023 m. liepos 19 d. nutarimu Nr. 576 „Dėl Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašo patvirtinimo“;

19.7. IT saugos atitikties vertinimo metodika;

19.8. Valstybės informacinių išteklių svarbos vertinimo metodika, patvirtinta Lietuvos Respublikos ekonomikos ir inovacijų ministro 2023 m. liepos 19 d. įsakymu Nr. 4-418 „Dėl Valstybės informacinių išteklių svarbos vertinimo metodikos patvirtinimo“;

19.9. Lietuvos standartai LST ISO/IEC 27002 ir LST ISO/IEC 27001, Lietuvos ir tarptautiniai „Informacinės technologijos. Saugumo metodai“ grupės standartai, nustatantys saugų informacinės sistemos duomenų tvarkymą;

19.10. registro nuostatai;

19.11. Saugos nuostatai;

19.12. saugos politikos įgyvendinamieji dokumentai.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

20. Vadovaujantis Metodikos 8.5.3 papunkčiu, registre tvarkoma elektroninė informacija priskiriama vidutinės svarbos valstybės informaciniams ištekliams.

21. Saugos įgaliotinis, atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacinės technologijos. Saugumo metodai“ grupės standartus, kasmet organizuoja registro rizikos įvertinimą, jeigu teisės aktai nenustato kitaip. Prireikus saugos įgaliotinis gali organizuoti neeilinį registro rizikos įvertinimą. Neeilinis registro rizikos įvertinimas atliekamas pasikeitus registro struktūrai (esminiai registro funkciniai pakitimai ir programinės įrangos keitimas), įvykus dideliems Administracijos organizaciniams pokyčiams, atsiradus naujų informacinių technologijų saugos srities reikalavimų, po saugos incidento, kurio metu buvo sutrikdyta registro veikla, sugadinta ar prarasta registre tvarkoma elektroninė informacija.

22. Registro rizikos įvertinimas atliekamas pagal kokybinį rizikos vertinimo metodą. Kartu su pagrindiniu registro rizikos įvertinimu organizuojamas ir atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos registro kibernetiniam saugumui, vertinimas. Administracijos vadovo rašytiniu pavedimu registro rizikos įvertinimą gali atlikti pats saugos įgaliotinis. Rizikos įvertinimui atlikti sutartiniais pagrindais gali būti perkamos registro rizikos įvertinimo paslaugos iš trečiųjų asmenų.

23. Registro rizikos įvertinimo rezultatai pateikiami rizikos įvertinimo ataskaitoje ir ji pateikiama Administracijos vadovui. Registro rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos registro elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Registro rizikos įvertinimo ataskaitą rengia arba, jei įvertinimą atlieka tretieji asmenys, dalyvauja rengiant saugos įgaliotinis. Svarbiausi rizikos veiksniai yra šie:

23.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai

elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);

23.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis registro elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

23.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

24. Rizikos įvertinimo metu atliekamos veiklos:

24.1. registrą sudarančių informacinių išteklių inventorizacija;

24.2. įtakos registro veiklai vertinimas;

24.3. grėsmės ir pažeidimų analizė;

24.4. liekamosios rizikos vertinimas.

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

26. Kibernetinio saugumo atitikties reikalavimams vertinimo metu taip pat turi būti atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos informacinių sistemų kibernetiniam saugumui, vertinimas, kurio metu imituojamos kibernetinės atakos ir vykdomos kibernetinių incidentų imitavimo pratybos. Kibernetinių atakų imitavimo etapai:

26.1. Planavimas. Parengiamas pažeidžiamumų nustatymo planas, kuriame apibrėžiami kibernetinių atakų imitavimo tikslai ir darbų apimtis, pateikiamas darbų grafikas, aprašomi planuojamų imituoti kibernetinių atakų tipai (išorinės ir (ar) vidinės), kibernetinių atakų imitavimo būdai (juodosios dėžės (angl. *Black Box*), baltosios dėžės (angl. *White Box*) ir (ar) pilkosios dėžės (angl. *Grey Box*), galima neigiama įtaka veiklai, kibernetinių atakų imitavimo metodologija, programiniai ir (ar) techniniai įrankiai ir priemonės, naudojami pažeidžiamumams nustatyti, nurodomos už pažeidžiamumų nustatymo plano vykdymą atsakingų asmenų teisės ir pareigos.

26.2. Žvalgyba (angl. *Reconnaissance*) ir aptikimas (angl. *Discovery*). Surenkama informacija apie perimetrą, tinklo mazgus, tinklo mazguose veikiančių tarnybinių stočių ir kitų tinklo įrenginių operacines sistemas ir programinę įrangą, paslaugas (angl. *Services*), pažeidžiamumą, konfigūracijas ir kitą sėkmingai kibernetinei atakai įvykdyti reikalingą informaciją.

26.3. Kibernetinių atakų imitavimas. Atliekami pažeidžiamumų nustatymo plane numatyti testai.

26.4. Ataskaitos parengimas. Kibernetinių atakų imitavimo rezultatai turi būti pateikti kibernetinio saugumo atitikties reikalavimams vertinimo ataskaitoje. Pažeidžiamumų nustatymo plane numatyti testų rezultatai turi būti detalizuojami ataskaitoje ir lyginami su planuotais. Kiekvienas aptiktas pažeidžiamumas turi būti detalizuojamas ir pateikiamos rekomendacijos jam pašalinti. Kibernetinių atakų imitavimo rezultatai turi būti pagrįsti patikimais įrodymais ir rizikos įvertinimu. Jeigu nustatoma incidentų valdymo ir šalinimo, taip pat organizacijos nepertraukiamos veiklos užtikrinimo trūkumų, turi būti tobulinami veiklos tęstinumo planai.

27. Atsižvelgiant į kibernetinio saugumo atitikties reikalavimams vertinimo ataskaitą, rengiamas nustatytų trūkumų šalinimo planas, kuriame, atsižvelgiant į kibernetinių atakų imitavimo metu nustatytus trūkumus, registro valdytojo vadovui teikiami pasiūlymai dėl kibernetinį saugumą reglamentuojančių teisės aktų ar kitų registro valdytojo vadovo patvirtintų dokumentų pakeitimo, kibernetinio saugumo būklės gerinimo ir papildomų kibernetinio saugumo priemonių įsigijimo. Nustatytų trūkumų šalinimo planą tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato registro valdytojo vadovas.

28. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas, kibernetinio saugumo atitikties reikalavimams vertinimo ataskaitos ir nustatytų

trūkumų šalinimo plano kopijas registro valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai (toliau – ARSIS) Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“ (toliau – Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatai) nustatyta tvarka.

29. Siekdamas užtikrinti Saugos nuostatų ir saugos politikos įgyvendinamųjų dokumentų nuostatų įgyvendinimo kontrolę, saugos įgaliotinis ne rečiau kaip kartą per metus, jeigu teisės aktai nenustato kitaip, organizuoja informacinių technologijų saugos atitikties vertinimą pagal IT saugos atitikties vertinimo metodikos reikalavimus.

30. Atliekant registro informacinių technologijų saugos atitikties vertinimą:

30.1. įvertinama esamos registro elektroninės informacijos saugos situacijos atitiktis registro saugos dokumentams ir kitiems elektroninės informacijos saugą reglamentuojantiems teisės aktams;

30.2. inventorizuojama registro techninė ir programinė įranga;

30.3. peržiūrima ir įvertinama registro administratoriui, registro paslaugos teikėjo administratoriui, registro naudotojams suteiktų teisių atitiktis jų atliekamoms funkcijoms;

30.4. duomenų saugos požiūriu patikrinama registro techninė ir programinė įranga: visos tarnybinės stotys ir ne mažiau kaip 10 proc. atsitiktinai parinktų registro naudotojų kompiuterinių darbo vietų (toliau – KDV);

30.5. įvertinamas pasirengimas užtikrinti registro veiklos tęstinumą įvykus saugos incidentui.

31. Atlikus registro informacinių technologijų saugos atitikties vertinimą, parengiama informacinių technologijų saugos atitikties vertinimo ataskaita ir pateikiama Administracijos vadovui, taip pat parengiamas pastebėtų trūkumų šalinimo planas. Registro valdytojo vadovas patvirtina šį planą, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminus.

32. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas registro valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti ARSIS Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

33. Prireikus saugos įgaliotinis gali organizuoti neeilinį registro informacinių technologijų saugos atitikties vertinimą.

34. Neeilinis registro informacinių technologijų saugos atitikties vertinimas atliekamas:

34.1. įvykus registro techninės ar programinės įrangos pokyčiams, kurie gali turėti įtakos registro veikimui;

34.2. paaiškėjus naujoms tendencijoms informacinių technologijų saugos srityje, dėl kurių kiltų grėsmė registro techninei, programinei įrangai ar registro tvarkomai elektroninei informacijai;

34.3. po saugos incidento, kurio metu buvo sutrikdyta registro veikla, sugadinta ar prarasta registro elektroninė informacija.

35. Techninės, programinės ir organizacinės registro elektroninės informacijos saugos priemonės pasirenkamos atsižvelgiant į registro valdytojo ir Administracijos turimus išteklius, vadovaujantis šiais priemonių parinkimo principais:

35.1. Liekamoji rizika turi būti sumažinta iki priimtino lygio.

35.2. Informacijos saugos priemonės diegimo kaina turi būti adekvati saugomos informacijos vertei.

35.3. Esant galimybei, turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

36. 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 eksploatuojamo registro.

37. Registro pokyčius gali inicijuoti saugos įgaliotinis ar registro administratorius, o įgyvendina registro administratorius.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

38. Nustatomi šie registro naudojamos programinės įrangos reikalavimai:

38.1. Registro naudojama programinė įranga turi atitikti programinės įrangos saugos gerąją praktiką, kuriant programinę įrangą taikomą saugos gerąją praktiką, programinės įrangos kūrimo struktūras, standartus.

38.2. Specifiniai saugos reikalavimai turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose.

38.3. Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos.

38.4. Programinės įrangos kūrimo, testavimo ir verifikacijos etapai turi vykti atsižvelgiant į pagrindinius saugos reikalavimus.

38.5. Prieš pradedant naudoti programinę įrangą, turi būti atliktas šios programinės įrangos pažeidžiamumo, pritaikomumo ir infrastruktūros atsparumo skverbimuisi įvertinimas. Programinė įranga negali būti patvirtinta, kol nėra pasiektas reikiamas saugumo lygis.

38.6. Turi būti atliekami periodiški infrastruktūros atsparumo skverbimuisi testavimai.

39. Programinės įrangos, skirtos registrui ir KDV apsaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos:

39.1. Registre turi būti naudojama antivirusinė programinė įranga, skirta registrui apsaugoti nuo kenksmingos programinės įrangos.

39.2. Antivirusinė programinė įranga turi būti atnaujinama automatiškai ne rečiau kaip kartą per parą.

39.3. Registro naudotojų kompiuteriuose naudojama įranga, skirta KDV apsaugoti nuo kenksmingos programinės įrangos, turi apsaugoti ir elektroninio pašto programinę įrangą nuo nepageidaujamo pašto ar kenksmingų programų patekimo į KDV.

39.4. Atsiradus požymių, kad KDV yra kenksmingų programų, turi būti patikrinami visi KDV standieji diskai, naudojama programinė įranga, skirta registrui ir KDV apsaugoti nuo kenksmingos programinės įrangos.

39.5. KDV esančios programinės įrangos, skirtos registrui ir KDV apsaugoti nuo kenksmingos programinės įrangos, nustatymai turi būti parinkti pagal rekomenduojamus tokios programinės įrangos gamintojų reikalavimus arba pagal vidinio kompiuterių tinklo administratoriaus rekomendacijas.

39.6. Programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

39.7. Apsaugos sistema privalo automatiškai informuoti registro paslaugos teikėjo administratorių apie KDV ir tarnybines stotis, kuriose apsaugos sistema netinkamai funkcionuoja, yra išjungta arba neatsinaujino per 24 valandas.

39.8. Registro operacinės sistemos ir naudojami programinės įrangos gamintojų rekomenduojami atnaujinimai turi būti įdiegiami nedelsiant, nesutrikdant registro paslaugų teikimo ir suderinus atnaujinimų darbus su registro administratoriumi.

39.9. Registro naudotojų kompiuterių apsaugos priemonės yra valdomos (ugniasienių įjungimas ir konfigūravimas, antivirusinių programų ir operacinių sistemų atnaujinimas) centralizuotai.

40. Metodai ir priemonės, kurie taikomi užtikrinant prieigą prie registro:

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

40.2. Registro priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą administratoriaus klasifikatorių, kuriuo naudojantis nebūtų galima atlikti registro naudotojo funkcijų.

40.3. Registro naudotojas turi būti registre unikaliai identifikuojamas – registro naudotojas turi patvirtinti savo tapatybę slaptažodžiu, registro naudotojui suteiktas pirminis slaptažodis turi būti pakeistas pirmo prisijungimo metu. Slaptažodžiai sudaromi, keičiami ir jų galiojimo trukmė nustatoma vadovaujantis Lietuvos Respublikos jūrų laivų registro naudotojų administravimo taisyklėmis.

40.4. Prieigą prie registro suteikia, apriboja ir panaikina registro administratorius.

40.5. Teisė dirbti su konkrečia elektronine informacija suteikiama konkrečiam registro naudotojui.

40.6. Registro naudotojui teisė dirbti su konkrečia elektronine informacija turi būti ribojama ar sustabdoma, kai registro naudotojas neprisijungė ilgiau kaip 2 mėnesius, vykdomas registro naudotojo veiklos tyrimas ir pan. Pasibaigus valstybės tarnybos ar darbo santykiams, registro naudotojo teisė naudotis registru turi būti panaikinta.

40.7. Baigus darbą ar pasitraukiant iš darbo vietos, turi būti imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo registro, įjungiama ekrano užsklanda su slaptažodžiu, dokumentai padedami į pašaliniams asmenims neprieinamą vietą.

40.8. Registro naudotojui 15 min. neatliekant jokių veiksmų informacinėje sistemoje, registras turi užsirakinti, kad toliau naudotis registru būtų galima tik pakartojus tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus.

40.9. Prisijungimo prie kompiuterių tinklo laikas ir trukmė nėra ribojami, registras pasiekiamas visą parą.

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

41.1. Registre turi būti naudojama tik legali programinė įranga.

41.2. Draudžiama diegti ir naudoti bet kokią programinę įrangą, keisti sistemos, kompiuterio ar programinės įrangos sistemų nustatymus. Programinę įrangą, reikalingą registro naudotojo funkcijoms atlikti, KDV diegia, atnaujina, kontroliuoja ir prižiūri atsakingi Administracijos valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis, ar registro paslaugų teikėjo darbuotojai. Kiti asmenys (registro paslaugų teikėjų specialistai) gali diegti programinę įrangą tik suderinus su registro administratoriumi.

41.3. Diegti ir naudoti programinę įrangą, nesusijusią su registro valdytojo ar Administracijos veikla ar registro naudotojo atliekamomis funkcijomis (žaidimų, bylų siuntimo, internetinių pokalbių programas ir kt.), draudžiama.

41.4. Tarnybinėse stotyse ir registro naudotojų KDV privalo būti naudojama programinė įranga, kuri apsaugo nuo kenksmingos programinės įrangos ir kuri turi būti atnaujinama ne rečiau kaip kartą per parą laikantis gamintojo reikalavimų.

41.5. KDV, programinė įranga, jos sertifikatai ir licencijos kasmet turi būti inventorizuojami.

41.6. Naudojama programinė įranga, leidžianti atlikti registre naudojamų kompiuterių tinklų stebėseną ir užtikrinanti šių tinklų saugos prevencines priemones.

41.7. Programinė įranga yra nuolat atnaujinama laikantis gamintojo reikalavimų.

42. Leistinos kompiuterių (ypač nešiojamųjų) naudojimo ribos ir metodai, kuriais leidžiama užtikrinti saugų registro duomenų teikimą ir (ar) gavimą:

42.1. Stacionariuosiuose ir nešiojamuosiuose kompiuteriuose registro įjungimo metu turi būti identifikuojamas registro naudotojas.

42.2. Stacionarieji ir nešiojamieji registro naudotojų kompiuteriai privalo būti naudojami tik su tiesioginių pareigų atlikimu susijusiai veiklai. Iš kompiuterių, kurie perduodami remontui ar techninei priežiūrai, turi būti pašalinta visa neskelbtina registro elektroninė informacija.

42.3. Registro naudotojų nešiojamiesiems kompiuteriams ne Administracijos ar registro paslaugos teikėjo patalpose privaloma naudoti papildomas saugos priemones, kuriomis registro duomenys perduodami saugiu šifruotu virtualiu privačiu tinklu (angl. V*irtual Private Network*, toliau – VPN).

42.4. Registro naudotojai, darbinėms funkcijoms atlikti naudojantys nešiojamuosius kompiuterius, išnešdami juos iš Administracijos patalpų, norėdami registro elektroninę informaciją perduoti kompiuterių tinklais ne savo darbo vietoje, turi naudoti vieną iš išvardintų metodų: duomenų šifravimą, papildomą naudotojo tapatybės patvirtinimą, rakinimo įrenginį. Nešiojamojo kompiuterio pagrindinės įvesties ir išvesties sistema (BIOS) turi būti apsaugota slaptažodžiu ir nurodytas standusis diskas kaip pirminis paleidimo įrenginys. Iš išorės prie registro duomenų bazės prisijungimas ribojamas. Nešiojamuosiuose kompiuteriuose ar išorinėse kompiuterinėse laikmenose esantys duomenys turi būti šifruojami. Registro naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo.

43. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kt.) pagrindinės naudojimo nuostatos:

43.1. Techninis nuotolinio prisijungimo sprendimas turi užtikrinti ne žemesnį nei vidiniam prisijungimui naudojamą saugumo lygį, t. y. turi būti naudojamos Saugos nuostatuose minimos priemonės, duomenų perdavimas saugiu šifruotu VPN arba naudojant saugų duomenų perdavimo protokolą HTTPS (angl. *Hypertext Transfer Protocol Secure*).

43.2. Registro naudotojams, kuriems atliekant tiesiogines pareigas būtina prisijungti iš nutolusios darbo vietos, gali būti suteikiama nuotolinio prisijungimo prie registro galimybė.

43.3. Kompiuterinis tinklas, prie kurio prijungtos registro tarnybinės stotys ir registro naudotojų kompiuteriai, nuo viešojo interneto turi būti atskirtas ugniasienėmis ir įsilaužimų aptikimo ir prevencijos įranga, už kurios administravimą ir priežiūrą atsakingas registro paslaugos teikėjo administratorius.

43.4. Visas duomenų srautas į internetą ir iš jo yra filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos.

43.5. Naudojamos turinio filtravimo sistemos.

43.6. Naudojama programinė įranga, leidžianti atlikti registre naudojamų kompiuterių tinklų monitoringą ir užtikrinanti šių tinklų saugos prevencines priemones.

43.7. Registro tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių informacinės sistemos naudotojų kompiuterinę įrangą nuo kenksmingo kodo (naudojama antivirusinė programa).

43.8. Registro programinė įranga turi būti apsaugota nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS)*, dedikuoto atkirtimo nuo paslaugos (angl. *DDOS*) ir kitų. Pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project (OWASP*) interneto svetainėje www.owasp.org.

43.9. Už saugų registro kompiuterių tinklų veikimą pagal kompetenciją atsako Administracijos kompiuterių tinklų administratorius.

44. Užtikrinant saugų elektroninės informacijos teikimą kitoms valstybės institucijoms ir (ar) gavimą iš jų, naudojamas šifruotas VPN arba Saugus valstybinis duomenų perdavimo tinklas (toliau – SVDPT). Elektronine informacija keičiamasi per saugų duomenų perdavimo protokolą HTTPS žiniatinklio paslaugų metodu (XML formatu) arba duomenų bazių užklausomis. Duomenys teikiami ir (ar) gaunami automatizuotomis priemonėmis tik pagal duomenų teikimo sutartyje nustatytas specifikacijas, duomenų perdavimo sąlygas ir tvarką.

45. Metodai, kuriais gali būti užtikrinamas saugus registro elektroninės informacijos teikimas ir (ar) gavimas:

45.1. Iš registro duomenų teikėjų elektroninė informacija gaunama pagal duomenų teikimo sutartyse numatytas elektroninės informacijos perdavimo technologijas, jų šifravimo mechanizmus, specifikacijas ir kitas sąlygas.

45.2. Duomenų gavėjų prieigą prie registro kontroliuoja kompiuterių tinklo užkarda.

45.3. Už registro elektroninės informacijos teikimo ir gavimo duomenų teikimo sutartyse nurodomų saugos reikalavimų nustatymą, suformulavimą ir įgyvendinimo organizavimą atsakingas saugos įgaliotinis.

45.4. Registro elektroninei informacijai perduoti naudojamas SVDPT arba kitas šifruotas perdavimo kanalas, užtikrinantis saugų elektroninės informacijos perdavimą.

46. Pagrindiniai atsarginių registro elektroninės informacijos kopijų (toliau – atsarginės kopijos) darymo ir atkūrimo reikalavimai:

46.1. Registro veiklos tęstinumui užtikrinti registro duomenys yra periodiškai, bet ne rečiau kaip kas 24 valandas kopijuojami į rezervinių kopijų laikmenas ir laikmenos saugomos taip, kad, įvykus saugos incidentui, visiškas registro funkcionalumas ir veikla būtų atkurti per 12 valandų.

46.2. Atsarginėms kopijoms kurti turi būti naudojama speciali programinė įranga.

46.3. Privalo būti visos saugomos elektroninės informacijos rezervinio kopijavimo funkcija.

46.4. Registro administratorius privalo turėti galimybę inicijuoti elektroninės informacijos atkūrimo iš rezervinės kopijos procedūrą pasirinktinai iš turimų rezervinių kopijų sąrašo. Atkūrus elektroninę informaciją privalo būti užtikrintas ir išlaikytas elektroninės informacijos vientisumas ir integralumas.

46.5. Registro elektroninė informacija registro naudotojams turi būti prieinama ne mažiau kaip 96 procentus sistemos veikimo laiko visą parą.

46.6. Elektroninė informacija atsarginėse kopijose turi būti šifruota (šifravimo raktai turi būti saugomi atskirai nuo atsarginių kopijų).

46.7. Atsarginės kopijos yra daromos ir saugomos taip, kad jos nebūtų prieinamos tretiesiems asmenims, kurie neturi teisės su jomis dirbti.

46.8. Atsarginės kopijos turi būti laikomos atskirai nuo tarnybinių stočių. Už atsarginių kopijų darymą, atkūrimą ir atkūrimo iš atsarginių kopijų testavimą yra atsakinga Administracija.

46.9. Atkūrimo iš atsarginių kopijų funkcija privalo būti išbandoma ne rečiau kaip kartą per pusmetį. Testavimo eiga ir rezultatai įforminami atsarginių kopijų darymo žurnale. Duomenų atkūrimo bandymą organizuoja saugos įgaliotinis.

47. Nustatomi duomenų naikinimo ir šalinimo reikalavimai:

47.1. Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinta visa joje esanti elektroninė informacija, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Jeigu to padaryti neįmanoma (pvz., DVD laikmenos), duomenų laikmenos turi būti fiziškai sunaikinamos be galimybės atkurti duomenis.

47.2. Prieš šalinant laikmenas, turi būti atlikti visų šalinamų laikmenų daugybiniai programinės įrangos perrašymai.

48. Jeigu saugiems duomenų naikinimo ir šalinimo duomenų laikmenose darbams atlikti yra pasitelkiamos trečiųjų asmenų paslaugos, turi būti sudaryta atitinkama paslaugų sutartis.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

49. Tvarkyti registro duomenis gali asmenys, susipažinę su Reglamentu (ES) 2016/679, registro nuostatais, registro saugos dokumentais, registrų ir informacinių sistemų saugos politiką reglamentuojančiais teisės aktais.

50. Registro naudotojai turi būti įgiję darbo kompiuteriu įgūdžių, mokėti tvarkyti registro elektroninę informaciją registro nuostatuose nurodyta tvarka, išmanyti registrų ir informacinių sistemų saugos politiką reglamentuojančius teisės aktus. Tvarkyti registro elektroninę informaciją gali tik registro naudotojai, pasirašę pasižadėjimą saugoti asmens duomenų paslaptį. Ši pareiga galioja perėjus dirbti į kitas pareigas arba pasibaigus valstybės tarnybos, darbo, sutartiniams ar kitiems santykiams.

51. Saugos įgaliotinis privalo išmanyti šiuolaikinių informacinių technologijų panaudojimo ypatumus, žinoti elektroninės informacijos saugos užtikrinimo principus bei metodus, rizikų valdymą, savo darbe vadovautis Reglamentu (ES) 2016/679, Aprašu, IT saugos atitikties vertinimo metodika, registro saugos dokumentais, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais elektroninės informacijos saugą, kibernetinę saugą, taip pat būti susipažinęs su esminiais registro elektroninės informacijos saugos reikalavimais. Saugos įgaliotinis privalo sugebėti prižiūrėti, kaip įgyvendinama saugos politika. Saugos įgaliotinis kiekvienais metais privalo tobulinti kvalifikaciją elektroninės informacijos saugos srityje.

52. Kibernetinio saugumo vadovas privalo išmanyti kibernetinio saugumo užtikrinimo principus, kiekvienais metais tobulinti kvalifikaciją kibernetinio saugumo srityje ir savo darbe vadovautis registro saugos dokumentais, Kibernetinio saugumo reikalavimų aprašu, Lietuvos Respublikos ir Europos Sąjungos teisės aktais, standartais, reglamentuojančiais kibernetinį saugumą.

53. Saugos įgaliotiniu ir kibernetinio saugumo vadovu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą galiojančią 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 nuobaudos paskyrimo praėję mažiau kaip vieni metai.

54. Registro administratorius ar registro paslaugos teikėjo administratorius privalo išmanyti darbą su kompiuterių tinklais ir mokėti užtikrinti jų saugumą, būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais, žinoti tarnybinių stočių veikimo principus, gebėti užtikrinti techninės ir programinės įrangos nepertraukiamą funkcionavimą bei saugą, stebėti techninės ir programinės įrangos veikimą, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, sutrikimų bei saugos incidentų diagnostiką ir šalinimą.

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

56. Registro naudotojų, registro administratoriaus ir registro paslaugos teikėjo administratoriaus mokymai organizuojami taip, kaip numatyta Saugos nuostatų 12.10 papunktyje, ne rečiau kaip kartą per metus. Mokymus organizuoja ir jų efektyvumą vertina saugos įgaliotinis.

V SKYRIUS
REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

57. Registro naudotojų, registro administratoriaus ir registro paslaugos teikėjo administratoriaus supažindinimą su registro saugos dokumentais ar kitais elektroninės informacijos saugą reglamentuojančiais teisės aktais ir atsakomybe, kylančia dėl jų pažeidimo,

atlieka saugos įgaliotinis pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodymą.

58. Registro administratorių ir registro paslaugos teikėjo administratorių su registro saugos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodymą, supažindina saugos įgaliotinis per 10 darbo dienų nuo registro administratoriaus ar registro paslaugos teikėjo administratoriaus paskyrimo.

59. Registro naudotojus su registro saugos dokumentais ir teisės aktais, reglamentuojančiais registro elektroninės informacijos saugą, saugos įgaliotinis pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodymą, supažindina prieš sukuriant registro naudotojo prisijungimo duomenis.

60. Pakartotinai su registro saugos dokumentais ir teisės aktais, reglamentuojančiais registro elektroninės informacijos saugą, saugos įgaliotinis pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodymą, supažindina registro naudotojus, registro administratorių ir registro paslaugos teikėjo administratorių kitą darbo dieną po registro saugos dokumentų ir teisės aktų, reglamentuojančių registro elektroninės informacijos saugą, priėmimo (išdėstymo nauja redakcija), pakeitimo ar pripažinimo netekusiais galios.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

61. Saugos įgaliotinis organizuoja registro saugos dokumentų persvarstymą ne rečiau kaip kartą per metus. Registro saugos dokumentai turi būti persvarstomi atlikus rizikos analizę ar informacinių technologijų saugos atitikties vertinimą, pasikeitus saugos politiką reglamentuojantiems teisės aktams, įvykus esminiams organizaciniams, technologiniams ar kitiems registro pokyčiams, po įvykusio kibernetinio incidento.

62. Saugos įgaliotinis, kibernetinio saugumo vadovas, registro administratorius, registro paslaugos teikėjo administratorius, registro naudotojai ir kiti subjektai, kuriems taikomi Saugos nuostatų reikalavimai, pažeidę registro saugos dokumentų ir kitų teisės aktų, reglamentuojančių saugų elektroninės informacijos tvarkymą, reikalavimus, atsako Lietuvos Respublikos teisės aktų, reguliuojančių valstybės registrų ir informacinių sistemų saugą, nustatyta tvarka.

_____

PATVIRTINTA
Lietuvos Respublikos susisiekimo ministro
2016 m. vasario 9 d. įsakymu Nr. 3-48(1.5 E)
(Lietuvos Respublikos susisiekimo ministro
2024 m. balandžio 19 d. įsakymo Nr. 3-138
redakcija)

LIETUVOS RESPUBLIKOS VIDAUS VANDENŲ LAIVŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos vidaus vandenų laivų registro duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Lietuvos Respublikos vidaus vandenų laivų registro (toliau – registras) elektroninės informacijos saugos politiką ir kibernetinio saugumo politiką (toliau – saugos politika), kurių tikslas – nustatyti ir įgyvendinti organizacines, administracines, technines ir kitas priemones, suteikiančias galimybę saugiai tvarkyti registro duomenis ir užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo netyčinio ar neteisėto sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jos.

2. Saugos nuostatuose vartojamos sąvokos suprantamos taip, kaip jos yra apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, 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 ir Saugos dokumentų turinio gairių aprašo patvirtinimo“ (toliau – Aprašas).

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

3.1. Lietuvos Respublikos vidaus vandenų laivų registro saugaus elektroninės informacijos tvarkymo taisyklės;

3.2. Lietuvos Respublikos vidaus vandenų laivų registro naudotojų administravimo taisyklės;

3.3. Lietuvos Respublikos vidaus vandenų laivų registro veiklos tęstinumo valdymo planas.

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

5. Registro elektroninės informacijos saugos ir kibernetinio saugumo (toliau – registro elektroninės informacijos sauga) užtikrinimo tikslai:

5.1. sudaryti sąlygas saugiai automatizuotomis priemonėmis tvarkyti registro elektroninę informaciją;

5.2. užtikrinti registro elektroninės informacijos patikimumą, konfidencialumą, prieinamumą, vientisumą ir tinkamą techninės, programinės ir ryšių įrangos funkcionavimą;

5.3. vykdyti elektroninės informacijos saugos ir kibernetinių incidentų (toliau – saugos incidentai), asmens duomenų saugumo pažeidimų prevenciją, reaguoti į saugos incidentus, asmens duomenų saugumo pažeidimus ir juos operatyviai suvaldyti.

6. Registro elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

6.1. registro elektroninei informacijai tvarkyti naudojamos techninės ir programinės įrangos kontrolė;

6.2. registro elektroninės informacijos tvarkymo kontrolė;

6.3. saugaus darbo su registro elektronine informacija kontrolė;

6.4. fizinė registro elektroninės informacijos tvarkymo priemonių (tarnybinių stočių, informacijos perdavimo įrangos, programinės įrangos) ir patalpų apsauga;

6.5. registro veiklos tęstinumas.

7. Registro valdytoja ir asmens duomenų valdytoja yra Lietuvos Respublikos susisiekimo ministerija, esanti adresu Gedimino pr. 17, 01103 Vilnius (toliau – registro valdytojas). Registro tvarkytoja ir asmens duomenų tvarkytoja yra Lietuvos transporto saugos administracija, esanti adresu Švitrigailos g. 42, 03209 Vilnius (toliau – Administracija).

8. Saugos nuostatais privalo vadovautis:

8.1. Administracijos valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis, registro saugos įgaliotinis (toliau – saugos įgaliotinis), registro administratorius, asmuo ar padalinys, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą (toliau – kibernetinio saugumo vadovas), registro duomenų valdymo įgaliotinis (toliau – duomenų valdymo įgaliotinis);

8.2. Administracijos Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka išrinkto juridinio asmens ar asmenų (asmenų grupės), kuriems Valstybės informacinių išteklių valdymo įstatymo 39 straipsnyje nustatytomis sąlygomis ir tvarka perduotos registro ir (ar) jo infrastruktūros priežiūros funkcijos (toliau – registro paslaugos teikėjas (-ai)), darbuotojai;

8.3. kiti subjektai, kuriems taikomi Saugos nuostatų reikalavimai.

9. Registro valdytojas atlieka šias funkcijas:

9.1. formuoja registro saugos politiką ir organizuoja jos įgyvendinimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą;

9.2. tvirtina registro saugos dokumentus, prižiūri ir kontroliuoja, kad registras būtų tvarkomas vadovaujantis šiais dokumentais, registro nuostatais ir kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą;

9.3. nagrinėja Administracijos pasiūlymus dėl registro elektroninės informacijos saugos tobulinimo ir priima dėl jų sprendimus;

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

9.5. atsižvelgdamas į kibernetinio saugumo atitikties reikalavimams vertinimo ataskaitą, prireikus tvirtina nustatytų trūkumų šalinimo planą;

9.6. priima sprendimą atlikti registro informacinių technologijų saugos atitikties vertinimą;

9.7. prireikus tvirtina registro informacinių technologijų saugos atitikties vertinimo metu pastebėtų trūkumų šalinimo planą;

9.8. įgyvendina registro pokyčius ir plėtrą;

9.9. pagal kompetenciją užtikrina registro elektroninės informacijos saugos priemones;

9.10. paveda Administracijai paskirti saugos įgaliotinį, duomenų valdymo įgaliotinį, registro administratorių, kibernetinio saugumo vadovą;

9.11. vykdo kitas registro saugos dokumentų ir kitų teisės aktų, reglamentuojančių saugų elektroninės informacijos tvarkymą, nustatytas funkcijas.

10. Administracija atlieka šias funkcijas:

10.1. įgyvendina reikiamas administracines, technines ir organizacines saugos priemones, užtikrina registro saugos reikalavimų atitiktį Saugos nuostatams ir saugos politikos įgyvendinamiesiems dokumentams;

10.2. skiria saugos įgaliotinį, duomenų valdymo įgaliotinį, kibernetinio saugumo vadovą ir registro administratorių;

10.3. rengia registro saugos dokumentus ir teikia juos tvirtinti registro valdytojui;

10.4. teikia registro valdytojui pasiūlymus dėl registro plėtros, saugos ir funkcionalumo;

10.5. organizuoja plėtrą ir registro pakeitimų įdiegimą;

10.6. rūpinasi registro elektroninės informacijos saugumu, užtikrina tinkamą registro administravimą ir nepertraukiamą registro veiklą;

10.7. koordinuoja ir kontroliuoja Administracijos valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartis, kurie naudoja registrą paskirtoms funkcijoms vykdyti, bei registro paslaugos teikėjo (-ų) darbuotojų (toliau kartu – registro naudotojai) veiklą;

10.8. užtikrina registro elektroninės informacijos tvarkymo teisėtumą, saugumą ir registro saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams ir registro saugos dokumentams;

10.9. atlieka kitas registro valdytojo pavestas, registro saugos dokumentuose bei teisės aktuose, reglamentuojančiuose saugų elektroninės informacijos tvarkymą, priskirtas funkcijas.

11. Registro paslaugos teikėjo (-ų) vadovas (-ai) paskiria administratorių (-ius) (toliau – registro paslaugos teikėjo administratorius), jis nurodomas Administracijos ir registro paslaugų teikėjo (-ų) sudarytoje (-ose) sutartyje (-yse).

12. Saugos įgaliotinis atlieka šias funkcijas:

12.1. teikia pasiūlymus Administracijos vadovui dėl:

12.1.1. registro administratoriaus paskyrimo ir reikalavimų jam nustatymo;

12.1.2. registro informacinių technologijų saugos atitikties vertinimo atlikimo, remiantis Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – IT saugos atitikties vertinimo metodika);

12.1.3. registro saugos dokumentų priėmimo, keitimo ar panaikinimo;

12.2. užtikrina tinkamą registro saugos reikalavimų ir funkcijų vykdymą;

12.3. organizuoja registro rizikos įvertinimą, prireikus – neeilinį registro rizikos įvertinimą ir registro informacinių technologijų saugos atitikties vertinimą;

12.4. informuoja pagal kompetenciją Administracijos vadovą apie registro saugos problemas;

12.5. teikia registro administratoriui, registro paslaugos teikėjo administratoriui, registro naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;

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

12.7. bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų saugos incidentus, neteisėtas veikas, susijusias su elektroninės informacijos sauga, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės;

12.8. užtikrina registro saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams;

12.9. pasirašytinai supažindina registro administratorių, registro paslaugos teikėjo administratorių ir registro naudotojus su registro saugos dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, ir atsakomybe už šių dokumentų reikalavimų nesilaikymą;

12.10. periodiškai inicijuoja registro administratoriaus, registro paslaugos teikėjo administratoriaus ir registro naudotojų mokymus elektroninės informacijos saugos klausimais, įvairiais būdais informuoja juos apie elektroninės informacijos saugos problemas (teminiai seminarai, atmintinės priimtiems naujiems darbuotojams ir pan.);

12.11. atlieka kitas Administracijos vadovo pavestas užduotis, registro saugos dokumentuose ir kituose saugos reikalavimus nustatančiuose teisės aktuose jam priskirtas funkcijas.

13. Saugos įgaliotinis negali atlikti registro administratoriaus funkcijų.

14. Registro administratorius atlieka šias funkcijas:

14.1. atlieka registro naudotojams priskirtų funkcijų ir suteiktų teisių atitikties vertinimą, administruoja šias teises;

14.2. rengia ir tikrina registro komponentų sąranką, teikia saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę, saugos politikos pažeidimus, nustatytas registro pažeidžiamas vietas;

14.3. ne rečiau kaip kartą per metus ir (arba) atlikus registro pakeitimus tikrina (peržiūri) registro komponentų sąranką ir registro būsenos rodiklius;

14.4. pagal kompetenciją rengia ir teikia Administracijos vadovui ir saugos įgaliotiniui pasiūlymus dėl registro kūrimo, palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

14.5. pagal kompetenciją reaguoja į saugos incidentus, registruoja juos ir informuoja apie juos saugos įgaliotinį, teikia pasiūlymus dėl minėtų incidentų šalinimo, taip pat informuoja saugos įgaliotinį apie nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones;

14.6. nustato registro pažeidžiamas vietas, vykdo saugumo reikalavimų atitikties stebėseną;

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

14.8. vykdo saugos įgaliotinio nurodymus ir pavedimus, susijusius su registro saugos politikos įgyvendinimu;

14.9. registruoja ir deaktyvuoja registro naudotojus, nustato prieigos prie registro teises;

14.10. užtikrina įdiegtą registro sąveiką su kitomis informacinėmis sistemomis ir registrais;

14.11. pagal kompetenciją administruoja techninės ir programinės įrangos, infrastruktūros bei informacinių technologijų paslaugas;

14.12. dalyvauja atkuriant registro elektroninę informaciją iš elektroninės informacijos atsarginių kopijų;

14.13. atlieka kitas registro saugos dokumentuose registro administratoriui priskirtas funkcijas ir vykdo kitus Administracijos vadovo nurodymus ir pavedimus, susijusius su registro užtikrinimu.

15. Administracija turi paskirti valstybės tarnautoją ar darbuotoją, dirbantį pagal darbo sutartį, kontroliuojantį registro paslaugos teikėjo administratorių.

16. Registro paslaugos teikėjo administratorius atlieka šias funkcijas:

16.1. reaguoja į saugos incidentus, registruoja juos ir informuoja registro administratorių apie nustatytus saugos politikos pažeidimus, teikia pasiūlymus dėl minėtų incidentų šalinimo, informuoja registro administratorių apie nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones;

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

16.3. vykdo registro paslaugos teikėjo darbuotojų, naudojančių registrą sutartiniams įsipareigojimams vykdyti, registre atliekamų veiksmų kontrolę;

16.4. atlieka kitas Administracijos ir registro paslaugos teikėjo sutartyje numatytas funkcijas, registro saugos dokumentuose registro paslaugos teikėjo administratoriui priskirtas funkcijas.

17. Kibernetinio saugumo vadovas atlieka šias funkcijas:

17.1. koordinuoja kibernetinių incidentų tyrimą, bendradarbiauja su kompetentingomis institucijomis, tiriančiomis kibernetinius incidentus;

17.2. atlieka kitas registro saugos dokumentuose nurodytas ir kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, jam priskirtas funkcijas.

18. Saugos įgaliotinis ir kibernetinio saugumo vadovas gali būti tas pats asmuo.

19. Teisės aktų, kuriais vadovaujamasi tvarkant registro elektroninę informaciją ir užtikrinant jos saugumą, sąrašas:

19.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

19.2. Valstybės informacinių išteklių valdymo įstatymas;

19.3. Kibernetinio saugumo įstatymas;

19.4. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“;

19.5. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Kibernetinio saugumo reikalavimų aprašas);

19.6. Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2023 m. liepos 19 d. nutarimu Nr. 576 „Dėl Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašo patvirtinimo“;

19.7. IT saugos atitikties vertinimo metodika;

19.8. Valstybės informacinių išteklių svarbos vertinimo metodika, patvirtinta Lietuvos Respublikos ekonomikos ir inovacijų ministro 2023 m. liepos 19 d. įsakymu Nr. 4-418 „Dėl Valstybės informacinių išteklių svarbos vertinimo metodikos patvirtinimo“;

19.9. Lietuvos standartai LST ISO/IEC 27002 ir LST ISO/IEC 27001, Lietuvos ir tarptautiniai „Informacinės technologijos. Saugumo metodai“ grupės standartai, nustatantys saugų informacinės sistemos duomenų tvarkymą;

19.10. registro nuostatai;

19.11. Saugos nuostatai;

19.12. saugos politikos įgyvendinamieji dokumentai.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

20. Vadovaujantis Metodikos 8.5.3 papunkčiu, registre tvarkoma elektroninė informacija priskiriama vidutinės svarbos valstybės informaciniams ištekliams.

21. Saugos įgaliotinis, atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacinės technologijos. Saugumo metodai“ grupės standartus, kasmet organizuoja registro rizikos įvertinimą, jeigu teisės aktai nenustato kitaip. Prireikus saugos įgaliotinis gali organizuoti neeilinį registro rizikos įvertinimą. Neeilinis registro rizikos įvertinimas atliekamas pasikeitus registro struktūrai (esminiai registro funkciniai pakitimai ir programinės įrangos keitimas), įvykus dideliems Administracijos organizaciniams pokyčiams, atsiradus naujų informacinių technologijų saugos srities reikalavimų, po saugos incidento, kurio metu buvo sutrikdyta registro veikla, sugadinta ar prarasta registre tvarkoma elektroninė informacija.

22. Registro rizikos įvertinimas atliekamas pagal kokybinį rizikos vertinimo metodą. Kartu su pagrindiniu registro rizikos įvertinimu organizuojamas ir atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos registro kibernetiniam saugumui, vertinimas. Administracijos vadovo rašytiniu pavedimu registro rizikos įvertinimą gali atlikti pats saugos įgaliotinis. Rizikos įvertinimui atlikti sutartiniais pagrindais gali būti perkamos registro rizikos įvertinimo paslaugos iš trečiųjų asmenų.

23. Registro rizikos įvertinimo rezultatai pateikiami rizikos įvertinimo ataskaitoje ir ji pateikiama Administracijos vadovui. Registro rizikos įvertinimo ataskaita rengiama atsižvelgiant

į rizikos veiksnius, galinčius turėti įtakos registro elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Registro rizikos įvertinimo ataskaitą rengia arba, jei įvertinimą atlieka tretieji asmenys, dalyvauja rengiant saugos įgaliotinis. Svarbiausi rizikos veiksniai yra šie:

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

23.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis registro elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

23.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

24. Rizikos įvertinimo metu atliekamos veiklos:

24.1. registrą sudarančių informacinių išteklių inventorizacija;

24.2. įtakos registro veiklai vertinimas;

24.3. grėsmės ir pažeidimų analizė;

24.4. liekamosios rizikos vertinimas.

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

26. Kibernetinio saugumo atitikties reikalavimams vertinimo metu taip pat turi būti atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos informacinių sistemų kibernetiniam saugumui, vertinimas, kurio metu imituojamos kibernetinės atakos ir vykdomos kibernetinių incidentų imitavimo pratybos. Kibernetinių atakų imitavimo etapai:

26.1. Planavimas. Parengiamas pažeidžiamumų nustatymo planas, kuriame apibrėžiami kibernetinių atakų imitavimo tikslai ir darbų apimtis, pateikiamas darbų grafikas, aprašomi planuojamų imituoti kibernetinių atakų tipai (išorinės ir (ar) vidinės), kibernetinių atakų imitavimo būdai (juodosios dėžės (angl. *Black Box*), baltosios dėžės (angl. *White Box*) ir (ar) pilkosios dėžės (angl. *Grey Box*), galima neigiama įtaka veiklai, kibernetinių atakų imitavimo metodologija, programiniai ir (ar) techniniai įrankiai ir priemonės, naudojami pažeidžiamumams nustatyti, nurodomos už pažeidžiamumų nustatymo plano vykdymą atsakingų asmenų teisės ir pareigos.

26.2. Žvalgyba (angl. *Reconnaissance*) ir aptikimas (angl. *Discovery*). Surenkama informacija apie perimetrą, tinklo mazgus, tinklo mazguose veikiančių tarnybinių stočių ir kitų tinklo įrenginių operacines sistemas ir programinę įrangą, paslaugas (angl. *Services*), pažeidžiamumą, konfigūracijas ir kitą sėkmingai kibernetinei atakai įvykdyti reikalingą informaciją.

26.3. Kibernetinių atakų imitavimas. Atliekami pažeidžiamumų nustatymo plane numatyti testai.

26.4. Ataskaitos parengimas. Kibernetinių atakų imitavimo rezultatai turi būti pateikti kibernetinio saugumo atitikties reikalavimams vertinimo ataskaitoje. Pažeidžiamumų nustatymo plane numatyti testų rezultatai turi būti detalizuojami ataskaitoje ir lyginami su planuotais. Kiekvienas aptiktas pažeidžiamumas turi būti detalizuojamas ir pateikiamos rekomendacijos jam pašalinti. Kibernetinių atakų imitavimo rezultatai turi būti pagrįsti patikimais įrodymais ir rizikos įvertinimu. Jeigu nustatoma incidentų valdymo ir šalinimo, taip pat organizacijos nepertraukiamos veiklos užtikrinimo trūkumų, turi būti tobulinami veiklos tęstinumo planai.

27. Atsižvelgiant į kibernetinio saugumo atitikties reikalavimams vertinimo ataskaitą, rengiamas nustatytų trūkumų šalinimo planas, kuriame, atsižvelgiant į kibernetinių atakų imitavimo metu nustatytus trūkumus, registro valdytojo vadovui teikiami pasiūlymai dėl kibernetinį saugumą reglamentuojančių teisės aktų ar kitų registro valdytojo vadovo patvirtintų dokumentų pakeitimo, kibernetinio saugumo būklės gerinimo ir papildomų kibernetinio saugumo priemonių įsigijimo. Nustatytų trūkumų šalinimo planą tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato registro valdytojo vadovas.

28. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas, kibernetinio saugumo atitikties reikalavimams vertinimo ataskaitos ir nustatytų trūkumų šalinimo plano kopijas registro valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai (toliau – ARSIS) Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“ (toliau – Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatai) nustatyta tvarka.

29. Siekdamas užtikrinti Saugos nuostatų ir saugos politikos įgyvendinamųjų dokumentų nuostatų įgyvendinimo kontrolę, saugos įgaliotinis ne rečiau kaip kartą per metus, jeigu teisės aktai nenustato kitaip, organizuoja informacinių technologijų saugos atitikties vertinimą pagal IT saugos atitikties vertinimo metodikos reikalavimus.

30. Atliekant registro informacinių technologijų saugos atitikties vertinimą:

30.1. įvertinama esamos registro elektroninės informacijos saugos situacijos atitiktis registro saugos dokumentams ir kitiems elektroninės informacijos saugą reglamentuojantiems teisės aktams;

30.2. inventorizuojama registro techninė ir programinė įranga;

30.3. peržiūrima ir įvertinama registro administratoriui, registro paslaugos teikėjo administratoriui, registro naudotojams suteiktų teisių atitiktis jų atliekamoms funkcijoms;

30.4. duomenų saugos požiūriu patikrinama registro techninė ir programinė įranga: visos tarnybinės stotys ir ne mažiau kaip 10 proc. atsitiktinai parinktų registro naudotojų kompiuterinių darbo vietų (toliau – KDV);

30.5. įvertinamas pasirengimas užtikrinti registro veiklos tęstinumą įvykus saugos incidentui.

31. Atlikus registro informacinių technologijų saugos atitikties vertinimą, parengiama informacinių technologijų saugos atitikties vertinimo ataskaita ir pateikiama Administracijos vadovui, taip pat parengiamas pastebėtų trūkumų šalinimo planas. Registro valdytojo vadovas patvirtina šį planą, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminus.

32. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas registro valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti ARSIS Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

33. Prireikus saugos įgaliotinis gali organizuoti neeilinį registro informacinių technologijų saugos atitikties vertinimą.

34. Neeilinis registro informacinių technologijų saugos atitikties vertinimas atliekamas:

34.1. įvykus registro techninės ar programinės įrangos pokyčiams, kurie gali turėti įtakos registro veikimui;

34.2. paaiškėjus naujoms tendencijoms informacinių technologijų saugos srityje, dėl kurių kiltų grėsmė registro techninei, programinei įrangai ar registro tvarkomai elektroninei informacijai;

34.3. po saugos incidento, kurio metu buvo sutrikdyta registro veikla, sugadinta ar prarasta registro elektroninė informacija.

35. Techninės, programinės ir organizacinės registro elektroninės informacijos saugos priemonės pasirenkamos atsižvelgiant į registro valdytojo ir Administracijos turimus išteklius, vadovaujantis šiais priemonių parinkimo principais:

35.1. Liekamoji rizika turi būti sumažinta iki priimtino lygio.

35.2. Informacijos saugos priemonės diegimo kaina turi būti adekvati saugomos informacijos vertei.

35.3. Esant galimybei, turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

36. 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 eksploatuojamo registro.

37. Registro pokyčius gali inicijuoti saugos įgaliotinis ar registro administratorius, o įgyvendina registro administratorius.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

38. Nustatomi šie registro naudojamos programinės įrangos reikalavimai:

38.1. Registro naudojama programinė įranga turi atitikti programinės įrangos saugos gerąją praktiką, kuriant programinę įrangą taikomą saugos gerąją praktiką, programinės įrangos kūrimo struktūras, standartus.

38.2. Specifiniai saugos reikalavimai turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose.

38.3. Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos.

38.4. Programinės įrangos kūrimo, testavimo ir verifikacijos etapai turi vykti atsižvelgiant į pagrindinius saugos reikalavimus.

38.5. Prieš pradedant naudoti programinę įrangą, turi būti atliktas šios programinės įrangos pažeidžiamumo, pritaikomumo ir infrastruktūros atsparumo skverbimuisi įvertinimas. Programinė įranga negali būti patvirtinta, kol nėra pasiektas reikiamas saugumo lygis.

38.6. Turi būti atliekami periodiški infrastruktūros atsparumo skverbimuisi testavimai.

39. Programinės įrangos, skirtos registrui ir KDV apsaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos:

39.1. Registre turi būti naudojama antivirusinė programinė įranga, skirta registrui apsaugoti nuo kenksmingos programinės įrangos.

39.2. Antivirusinė programinė įranga turi būti atnaujinama automatiškai ne rečiau kaip kartą per parą.

39.3. Registro naudotojų kompiuteriuose naudojama įranga, skirta KDV apsaugoti nuo kenksmingos programinės įrangos, turi apsaugoti ir elektroninio pašto programinę įrangą nuo nepageidaujamo pašto ar kenksmingų programų patekimo į KDV.

39.4. Atsiradus požymių, kad KDV yra kenksmingų programų, turi būti patikrinami visi KDV standieji diskai, naudojama programinė įranga, skirta registrui ir KDV apsaugoti nuo kenksmingos programinės įrangos.

39.5. KDV esančios programinės įrangos, skirtos registrui ir KDV apsaugoti nuo kenksmingos programinės įrangos, nustatymai turi būti parinkti pagal rekomenduojamus tokios programinės įrangos gamintojų reikalavimus arba pagal vidinio kompiuterių tinklo administratoriaus rekomendacijas.

39.6. Programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

39.7. Apsaugos sistema privalo automatiškai informuoti registro paslaugos teikėjo administratorių apie KDV ir tarnybines stotis, kuriose apsaugos sistema netinkamai funkcionuoja, yra išjungta arba neatsinaujino per 24 valandas.

39.8. Registro operacinės sistemos ir naudojami programinės įrangos gamintojų rekomenduojami atnaujinimai turi būti įdiegiami nedelsiant, nesutrikdant registro paslaugų teikimo ir suderinus atnaujinimų darbus su registro administratoriumi.

39.9. Registro naudotojų kompiuterių apsaugos priemonės yra valdomos (ugniasienių įjungimas ir konfigūravimas, antivirusinių programų ir operacinių sistemų atnaujinimas) centralizuotai.

40. Metodai ir priemonės, kurie taikomi užtikrinant prieigą prie registro:

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

40.2. Registro priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą administratoriaus klasifikatorių, kuriuo naudojantis nebūtų galima atlikti registro naudotojo funkcijų.

40.3. Registro naudotojas turi būti registre unikaliai identifikuojamas – registro naudotojas turi patvirtinti savo tapatybę slaptažodžiu, registro naudotojui suteiktas pirminis slaptažodis turi būti pakeistas pirmo prisijungimo metu. Slaptažodžiai sudaromi, keičiami ir jų galiojimo trukmė nustatoma vadovaujantis Lietuvos Respublikos vidaus vandenų laivų registro naudotojų administravimo taisyklėmis.

40.4. Prieigą prie registro suteikia, apriboja ir panaikina registro administratorius.

40.5. Teisė dirbti su konkrečia elektronine informacija suteikiama konkrečiam registro naudotojui.

40.6. Registro naudotojui teisė dirbti su konkrečia elektronine informacija turi būti ribojama ar sustabdoma, kai registro naudotojas neprisijungė ilgiau kaip 2 mėnesius, vykdomas registro naudotojo veiklos tyrimas ir pan. Pasibaigus valstybės tarnybos ar darbo santykiams, registro naudotojo teisė naudotis registru turi būti panaikinta.

40.7. Baigus darbą ar pasitraukiant iš darbo vietos, turi būti imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo registro, įjungiama ekrano užsklanda su slaptažodžiu, dokumentai padedami į pašaliniams asmenims neprieinamą vietą.

40.8. Registro naudotojui 15 min. neatliekant jokių veiksmų informacinėje sistemoje, registras turi užsirakinti, kad toliau naudotis registru būtų galima tik pakartojus tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus.

40.9. Prisijungimo prie kompiuterių tinklo laikas ir trukmė nėra ribojami, registras pasiekiamas visą parą.

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

41.1. Registre turi būti naudojama tik legali programinė įranga.

41.2. Draudžiama diegti ir naudoti bet kokią programinę įrangą, keisti sistemos, kompiuterio ar programinės įrangos sistemų nustatymus. Programinę įrangą, reikalingą registro naudotojo funkcijoms atlikti, KDV diegia, atnaujina, kontroliuoja ir prižiūri atsakingi Administracijos valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis, ar registro paslaugų teikėjo darbuotojai. Kiti asmenys (registro paslaugų teikėjų specialistai) gali diegti programinę įrangą tik suderinus su registro administratoriumi.

41.3. Diegti ir naudoti programinę įrangą, nesusijusią su registro valdytojo ar Administracijos veikla ar registro naudotojo atliekamomis funkcijomis (žaidimų, bylų siuntimo, internetinių pokalbių programas ir kt.), draudžiama.

41.4. Tarnybinėse stotyse ir registro naudotojų KDV privalo būti naudojama programinė įranga, kuri apsaugo nuo kenksmingos programinės įrangos ir kuri turi būti atnaujinama ne rečiau kaip kartą per parą laikantis gamintojo reikalavimų.

41.5. KDV, programinė įranga, jos sertifikatai ir licencijos kasmet turi būti inventorizuojami.

41.6. Naudojama programinė įranga, leidžianti atlikti registre naudojamų kompiuterių tinklų stebėseną ir užtikrinanti šių tinklų saugos prevencines priemones.

41.7. Programinė įranga yra nuolat atnaujinama laikantis gamintojo reikalavimų.

42. Leistinos kompiuterių (ypač nešiojamųjų) naudojimo ribos ir metodai, kuriais leidžiama užtikrinti saugų registro duomenų teikimą ir (ar) gavimą:

42.1. Stacionariuosiuose ir nešiojamuosiuose kompiuteriuose registro įjungimo metu turi būti identifikuojamas registro naudotojas.

42.2. Stacionarieji ir nešiojamieji registro naudotojų kompiuteriai privalo būti naudojami tik su tiesioginių pareigų atlikimu susijusiai veiklai. Iš kompiuterių, kurie perduodami remontui ar techninei priežiūrai, turi būti pašalinta visa neskelbtina registro elektroninė informacija.

42.3. Registro naudotojų nešiojamiesiems kompiuteriams ne Administracijos ar registro paslaugos teikėjo patalpose privaloma naudoti papildomas saugos priemones, kuriomis registro duomenys perduodami saugiu šifruotu virtualiu privačiu tinklu (angl. V*irtual Private Network*, toliau – VPN).

42.4. Registro naudotojai, darbinėms funkcijoms atlikti naudojantys nešiojamuosius kompiuterius, išnešdami juos iš Administracijos patalpų, norėdami registro elektroninę informaciją perduoti kompiuterių tinklais ne savo darbo vietoje, turi naudoti vieną iš išvardintų metodų: duomenų šifravimą, papildomą naudotojo tapatybės patvirtinimą, rakinimo įrenginį. Nešiojamojo kompiuterio pagrindinės įvesties ir išvesties sistema (BIOS) turi būti apsaugota slaptažodžiu ir nurodytas standusis diskas kaip pirminis paleidimo įrenginys. Iš išorės prie registro duomenų bazės prisijungimas ribojamas. Nešiojamuosiuose kompiuteriuose ar išorinėse kompiuterinėse laikmenose esantys duomenys turi būti šifruojami. Registro naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo.

43. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kt.) pagrindinės naudojimo nuostatos:

43.1. Techninis nuotolinio prisijungimo sprendimas turi užtikrinti ne žemesnį nei vidiniam prisijungimui naudojamą saugumo lygį, t. y. turi būti naudojamos Saugos nuostatuose minimos priemonės, duomenų perdavimas saugiu šifruotu VPN arba naudojant saugų duomenų perdavimo protokolą HTTPS (angl. *Hypertext Transfer Protocol Secure*).

43.2. Registro naudotojams, kuriems atliekant tiesiogines pareigas būtina prisijungti iš nutolusios darbo vietos, gali būti suteikiama nuotolinio prisijungimo prie registro galimybė.

43.3. Kompiuterinis tinklas, prie kurio prijungtos registro tarnybinės stotys ir registro naudotojų kompiuteriai, nuo viešojo interneto turi būti atskirtas ugniasienėmis ir įsilaužimų aptikimo ir prevencijos įranga, už kurios administravimą ir priežiūrą atsakingas registro paslaugos teikėjo administratorius.

43.4. Visas duomenų srautas į internetą ir iš jo yra filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos.

43.5. Naudojamos turinio filtravimo sistemos.

43.6. Naudojama programinė įranga, leidžianti atlikti registre naudojamų kompiuterių tinklų monitoringą ir užtikrinanti šių tinklų saugos prevencines priemones.

43.7. Registro tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių informacinės sistemos naudotojų kompiuterinę įrangą nuo kenksmingo kodo (naudojama antivirusinė programa).

43.8. Registro programinė įranga turi būti apsaugota nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS)*, dedikuoto atkirtimo nuo paslaugos (angl. *DDOS*) ir kitų. Pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project (OWASP*) interneto svetainėje www.owasp.org.

43.9. Už saugų registro kompiuterių tinklų veikimą pagal kompetenciją atsako Administracijos kompiuterių tinklų administratorius.

44. Užtikrinant saugų elektroninės informacijos teikimą kitoms valstybės institucijoms ir (ar) gavimą iš jų, naudojamas šifruotas VPN arba Saugus valstybinis duomenų perdavimo tinklas (toliau – SVDPT). Elektronine informacija keičiamasi per saugų duomenų perdavimo protokolą HTTPS žiniatinklio paslaugų metodu (XML formatu) arba duomenų bazių užklausomis. Duomenys teikiami ir (ar) gaunami automatizuotomis priemonėmis tik pagal duomenų teikimo sutartyje nustatytas specifikacijas, duomenų perdavimo sąlygas ir tvarką.

45. Metodai, kuriais gali būti užtikrinamas saugus registro elektroninės informacijos teikimas ir (ar) gavimas:

45.1. Iš registro duomenų teikėjų elektroninė informacija gaunama pagal duomenų teikimo sutartyse numatytas elektroninės informacijos perdavimo technologijas, jų šifravimo mechanizmus, specifikacijas ir kitas sąlygas.

45.2. Duomenų gavėjų prieigą prie registro kontroliuoja kompiuterių tinklo užkarda.

45.3. Už registro elektroninės informacijos teikimo ir gavimo duomenų teikimo sutartyse nurodomų saugos reikalavimų nustatymą, suformulavimą ir įgyvendinimo organizavimą atsakingas saugos įgaliotinis.

45.4. Registro elektroninei informacijai perduoti naudojamas SVDPT arba kitas šifruotas perdavimo kanalas, užtikrinantis saugų elektroninės informacijos perdavimą.

46. Pagrindiniai atsarginių registro elektroninės informacijos kopijų (toliau – atsarginės kopijos) darymo ir atkūrimo reikalavimai:

46.1. Registro veiklos tęstinumui užtikrinti registro duomenys yra periodiškai, bet ne rečiau kaip kas 24 valandas kopijuojami į rezervinių kopijų laikmenas ir laikmenos saugomos taip, kad, įvykus saugos incidentui, visiškas registro funkcionalumas ir veikla būtų atkurti per 12 valandų.

46.2. Atsarginėms kopijoms kurti turi būti naudojama speciali programinė įranga.

46.3. Privalo būti visos saugomos elektroninės informacijos rezervinio kopijavimo funkcija.

46.4. Registro administratorius privalo turėti galimybę inicijuoti elektroninės informacijos atkūrimo iš rezervinės kopijos procedūrą pasirinktinai iš turimų rezervinių kopijų sąrašo. Atkūrus elektroninę informaciją privalo būti užtikrintas ir išlaikytas elektroninės informacijos vientisumas ir integralumas.

46.5. Registro elektroninė informacija registro naudotojams turi būti prieinama ne mažiau kaip 96 procentus sistemos veikimo laiko visą parą.

46.6. Elektroninė informacija atsarginėse kopijose turi būti šifruota (šifravimo raktai turi būti saugomi atskirai nuo atsarginių kopijų).

46.7. Atsarginės kopijos yra daromos ir saugomos taip, kad jos nebūtų prieinamos tretiesiems asmenims, kurie neturi teisės su jomis dirbti.

46.8. Atsarginės kopijos turi būti laikomos atskirai nuo tarnybinių stočių. Už atsarginių kopijų darymą, atkūrimą ir atkūrimo iš atsarginių kopijų testavimą yra atsakinga Administracija.

46.9. Atkūrimo iš atsarginių kopijų funkcija privalo būti išbandoma ne rečiau kaip kartą per pusmetį. Testavimo eiga ir rezultatai įforminami atsarginių kopijų darymo žurnale. Duomenų atkūrimo bandymą organizuoja saugos įgaliotinis.

47. Nustatomi duomenų naikinimo ir šalinimo reikalavimai:

47.1. Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinta visa joje esanti elektroninė informacija, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Jeigu to padaryti neįmanoma (pvz., DVD laikmenos), duomenų laikmenos turi būti fiziškai sunaikinamos be galimybės atkurti duomenis.

47.2. Prieš šalinant laikmenas, turi būti atlikti visų šalinamų laikmenų daugybiniai programinės įrangos perrašymai.

48. Jeigu saugiems duomenų naikinimo ir šalinimo duomenų laikmenose darbams atlikti yra pasitelkiamos trečiųjų asmenų paslaugos, turi būti sudaryta atitinkama paslaugų sutartis.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

49. Tvarkyti registro duomenis gali asmenys, susipažinę su Reglamentu (ES) 2016/679, registro nuostatais, registro saugos dokumentais, registrų ir informacinių sistemų saugos politiką reglamentuojančiais teisės aktais.

50. Registro naudotojai turi būti įgiję darbo kompiuteriu įgūdžių, mokėti tvarkyti registro elektroninę informaciją registro nuostatuose nurodyta tvarka, išmanyti registrų ir informacinių sistemų saugos politiką reglamentuojančius teisės aktus. Tvarkyti registro elektroninę informaciją gali tik registro naudotojai, pasirašę pasižadėjimą saugoti asmens duomenų paslaptį. Ši pareiga galioja perėjus dirbti į kitas pareigas arba pasibaigus valstybės tarnybos, darbo, sutartiniams ar kitiems santykiams.

51. Saugos įgaliotinis privalo išmanyti šiuolaikinių informacinių technologijų panaudojimo ypatumus, žinoti elektroninės informacijos saugos užtikrinimo principus bei metodus, rizikų valdymą, savo darbe vadovautis Reglamentu (ES) 2016/679, Aprašu, IT saugos atitikties vertinimo metodika, registro saugos dokumentais, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais elektroninės informacijos saugą, kibernetinę saugą, taip pat būti susipažinęs su esminiais registro elektroninės informacijos saugos reikalavimais. Saugos įgaliotinis privalo sugebėti prižiūrėti, kaip įgyvendinama saugos politika. Saugos įgaliotinis kiekvienais metais privalo tobulinti kvalifikaciją elektroninės informacijos saugos srityje.

52. Kibernetinio saugumo vadovas privalo išmanyti kibernetinio saugumo užtikrinimo principus, kiekvienais metais tobulinti kvalifikaciją kibernetinio saugumo srityje ir savo darbe vadovautis registro saugos dokumentais, Kibernetinio saugumo reikalavimų aprašu, Lietuvos Respublikos ir Europos Sąjungos teisės aktais, standartais, reglamentuojančiais kibernetinį saugumą.

53. Saugos įgaliotiniu ir kibernetinio saugumo vadovu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą galiojančią 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 nuobaudos paskyrimo praėję mažiau kaip vieni metai.

54. Registro administratorius ar registro paslaugos teikėjo administratorius privalo išmanyti darbą su kompiuterių tinklais ir mokėti užtikrinti jų saugumą, būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais, žinoti tarnybinių stočių veikimo principus, gebėti užtikrinti techninės ir programinės įrangos nepertraukiamą funkcionavimą bei saugą, stebėti techninės ir programinės įrangos veikimą, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, sutrikimų bei saugos incidentų diagnostiką ir šalinimą.

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

56. Registro naudotojų, registro administratoriaus ir registro paslaugos teikėjo administratoriaus mokymai organizuojami taip, kaip numatyta Saugos nuostatų 12.10 papunktyje, ne rečiau kaip kartą per metus. Mokymus organizuoja ir jų efektyvumą vertina saugos įgaliotinis.

V SKYRIUS
REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

57. Registro naudotojų, registro administratoriaus ir registro paslaugos teikėjo administratoriaus supažindinimą su registro saugos dokumentais ar kitais elektroninės informacijos saugą reglamentuojančiais teisės aktais ir atsakomybe, kylančia dėl jų pažeidimo, atlieka saugos įgaliotinis pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodymą.

58. Registro administratorių ir registro paslaugos teikėjo administratorių su registro saugos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodymą, supažindina saugos įgaliotinis per 10 darbo dienų nuo registro administratoriaus ar registro paslaugos teikėjo administratoriaus paskyrimo.

59. Registro naudotojus su registro saugos dokumentais ir teisės aktais, reglamentuojančiais registro elektroninės informacijos saugą, saugos įgaliotinis pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodymą, supažindina prieš sukuriant registro naudotojo prisijungimo duomenis.

60. Pakartotinai su registro saugos dokumentais ir teisės aktais, reglamentuojančiais registro elektroninės informacijos saugą, saugos įgaliotinis pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodymą, supažindina registro naudotojus, registro administratorių ir registro paslaugos teikėjo administratorių kitą darbo dieną po registro saugos dokumentų ir teisės aktų, reglamentuojančių registro elektroninės informacijos saugą, priėmimo (išdėstymo nauja redakcija), pakeitimo ar pripažinimo netekusiais galios.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

61. Saugos įgaliotinis organizuoja registro saugos dokumentų persvarstymą ne rečiau kaip kartą per metus. Registro saugos dokumentai turi būti persvarstomi atlikus rizikos analizę ar informacinių technologijų saugos atitikties vertinimą, pasikeitus saugos politiką reglamentuojantiems teisės aktams, įvykus esminiams organizaciniams, technologiniams ar kitiems registro pokyčiams, po įvykusio kibernetinio incidento.

62. Saugos įgaliotinis, kibernetinio saugumo vadovas, registro administratorius, registro paslaugos teikėjo administratorius, registro naudotojai ir kiti subjektai, kuriems taikomi Saugos nuostatų reikalavimai, pažeidę registro saugos dokumentų ir kitų teisės aktų, reglamentuojančių saugų elektroninės informacijos tvarkymą, reikalavimus, atsako Lietuvos Respublikos teisės aktų, reguliuojančių valstybės registrų ir informacinių sistemų saugą, nustatyta tvarka.

_____

Pakeitimai:

1.
Lietuvos Respublikos susisiekimo ministerija, Įsakymas
Nr. 3-138, 2024-04-19, paskelbta TAR 2024-04-19, i. k. 2024-07254
Dėl Lietuvos Respublikos susisiekimo ministro 2016 m. vasario 9 d. įsakymo Nr. 3-48(1.5 E) „Dėl Lietuvos saugios laivybos administracijos tvarkomų registrų duomenų saugos nuostatų patvirtinimo“ pakeitimo