Suvestinė redakcija nuo 2021-03-02

Įsakymas paskelbtas: Žin. 2012, Nr. 82-4316, i. k. 11223IRISAK0005V-57

Nauja redakcija nuo 2021-03-02:
Nr. 5V-21, 2021-02-26, paskelbta TAR 2021-03-01, i. k. 2021-04022

INFORMATIKOS IR RYŠIŲ DEPARTAMENTO PRIE LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS DIREKTORIUS

ĮSAKYMAS DĖL ĮTARIAMŲJŲ, KALTINAMŲJŲ IR NUTEISTŲJŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2012 m. liepos 4 d. Nr. 5V-57
Vilnius

Vadovaudamasi Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 43 straipsnio 2 dalimi, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 7.1 papunkčiu, 11, 19 ir 26 punktais ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, 5.3 papunkčiu:

1. T v i r t i n u Įtariamųjų, kaltinamųjų ir nuteistųjų registro duomenų saugos nuostatus (pridedama).

2. N u r o d a u, užtikrinant duomenų ir informacijos, tvarkomos Įtariamųjų, kaltinamųjų ir nuteistųjų registre, saugą ir kibernetinį saugumą, *mutatis mutandis* vadovautis Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėmis, Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų naudotojų administravimo taisyklėmis ir Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų veiklos tęstinumo valdymo planu, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2018 m. lapkričio 26 d. įsakymu Nr. 1V-871 „Dėl Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklių, naudotojų administravimo taisyklių ir veiklos tęstinumo valdymo plano patvirtinimo“.

DIREKTORIUS GINTARAS ČIURLIONIS

PATVIRTINTA
Informatikos ir ryšių departamento prie
Lietuvos Respublikos vidaus reikalų
ministerijos direktoriaus
2012 m. liepos 4 d. įsakymu Nr. 5V-57
(Informatikos ir ryšių departamento prie
Lietuvos Respublikos vidaus reikalų
ministerijos direktoriaus
2021 m. vasario 26 d. įsakymo Nr. 5V-21
redakcija)

ĮTARIAMŲJŲ, KALTINAMŲJŲ IR NUTEISTŲJŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Įtariamųjų, kaltinamųjų ir nuteistųjų registro duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Įtariamųjų, kaltinamųjų ir nuteistųjų registro (toliau – Registras) duomenų saugos politiką ir kibernetinio saugumo politiką (toliau – Registro duomenų saugos politika), kurios tikslas – nustatyti ir įgyvendinti organizacines, technines ir kitas priemones, suteikiančias galimybę saugiai tvarkyti Registro duomenis, Registro informaciją, Registrui pateiktus dokumentus ir (arba) jų kopijas (toliau – Registro duomenys) ir užtikrinti, kad Registro duomenys būtų patikimi ir apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo ar neteisėto jų tvarkymo.

2. Registro duomenų saugos politika įgyvendinama pagal Registro duomenų saugos politiką įgyvendinančius dokumentus: Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų saugaus elektroninės informacijos tvarkymo taisykles, Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų naudotojų administravimo taisykles ir Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų veiklos tęstinumo valdymo planą, patvirtintus Lietuvos Respublikos vidaus reikalų ministro 2018 m. lapkričio 26 d. įsakymu Nr. 1V-871 „Dėl Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklių, naudotojų administravimo taisyklių ir veiklos tęstinumo valdymo plano patvirtinimo“, (toliau – saugos politiką įgyvendinantys dokumentai).

3. Saugos nuostatuose vartojamos sąvokos atitinka 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, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas) ir Įtariamųjų, kaltinamųjų ir nuteistųjų registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2012 m. balandžio 18 d. nutarimu Nr. 435 „Dėl Įtariamųjų, kaltinamųjų ir nuteistųjų registro nuostatų patvirtinimo“, (toliau – Registro nuostatai) vartojamas sąvokas.

4. Registro duomenų saugos ir kibernetinio saugumo (toliau – Registro duomenų sauga) tikslas – užtikrinti Registro duomenų konfidencialumą, prieinamumą bei vientisumą ir sudaryti sąlygas saugiai automatiniu būdu tvarkyti Registro duomenis.

5. Registro duomenų saugos užtikrinimo prioritetinės kryptys:

5.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų Registro duomenų saugai užtikrinti, įgyvendinimas ir kontrolė;

5.2. Registro veiklos tęstinumo užtikrinimas;

5.3. Registre tvarkomų asmens duomenų apsauga.

6. Registro duomenų saugai užtikrinti kompleksiškai naudojamos administracinės, techninės ir programinės priemonės.

7. Saugos nuostatai ir saugos politiką įgyvendinantys dokumentai taikomi:

7.1. Registro valdytojui ir tvarkytojui – Informatikos ir ryšių departamentui prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Informatikos ir ryšių departamentas) (Šventaragio g. 2, Vilnius);

7.2. Registro saugos įgaliotiniui (toliau – saugos įgaliotinis);

7.3. Registro administratoriams;

7.4. Registro naudotojams;

7.5. paslaugų, darbų ir įrangos, susijusių su Registru, teikėjams.

8. Registro naudotojai, tvarkantys Registro duomenis, privalo įsipareigoti saugoti Registro duomenų paslaptį. Įsipareigojimas saugoti Registro duomenų paslaptį galioja ir nutraukus su Registro duomenų tvarkymu susijusią veiklą.

9. Paslaugų, darbų ir įrangos, susijusių su Registru, teikėjai privalo įsipareigoti saugoti Registro duomenų paslaptį ir pasirašyti konfidencialumo pasižadėjimą. Įsipareigojimas saugoti Registro duomenų paslaptį galioja ir pasibaigus paslaugų teikimo laikui ar nutraukus šią veiklą.

10. Registro valdytojas atsako už Registro duomenų saugos politikos formavimą, jos įgyvendinimo organizavimą ir priežiūrą, Registro duomenų tvarkymo bei duomenų teikimo duomenų gavėjams teisėtumą.

11. Registro valdytojo funkcijos:

11.1. rengia ir priima teisės aktus, susijusius su Registro duomenų tvarkymu ir sauga, kontroliuoja, kaip jų laikomasi;

11.2. priima sprendimus dėl Registrui taikomų informacinių technologijų saugos atitikties vertinimo atlikimo;

11.3. atsižvelgdamas į informacinių technologijų saugos atitikties vertinimo ataskaitą, prireikus tvirtina trūkumų šalinimo planą;

11.4. užtikrina Registro funkcijų pokyčių valdymo planavimą;

11.5. skiria saugos įgaliotinį ir Registro administratorius;

11.6. atlieka kitas Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, (toliau − Kibernetinio saugumo reikalavimų aprašas), Registro nuostatuose, saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose nustatytas funkcijas, susijusias su Registro duomenų sauga.

12. Informatikos ir ryšių departamento, kaip Registro tvarkytojo, funkcijos:

12.1. užtikrina Registro duomenų tvarkymo teisėtumą ir saugų Registro duomenų perdavimą kompiuterių tinklais (automatiniu būdu);

12.2. atlieka kitas Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, Registro nuostatuose, saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose nustatytas funkcijas, susijusias su Registro duomenų sauga.

13. Saugos įgaliotinio funkcijos:

13.1. teikia Registro valdytojo vadovui pasiūlymus dėl:

13.1.1. Registro administratorių paskyrimo;

13.1.2. Registro informacinių technologijų saugos atitikties vertinimo atlikimo Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 43 punkte nurodytoje metodikoje nustatyta tvarka;

13.1.3. Saugos nuostatų ir saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

13.2. koordinuoja Registro duomenų saugos ir kibernetinių incidentų (toliau – saugos incidentai) tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų incidentus, saugos incidentus, neteisėtas veikas, susijusias su elektroninės informacijos sauga;

13.3. teikia Registro administratoriams ir Registro naudotojams privalomus vykdyti nurodymus ir pavedimus dėl Registro saugos politikos įgyvendinimo;

13.4. organizuoja Registro saugos rizikos vertinimą;

13.5. kartą per metus organizuoja Registro naudotojų elektroninės informacijos saugos mokymą, įvairiais būdais informuoja juos apie elektroninės informacijos saugos aktualijas;

13.6. įgyvendindamas Registro duomenų saugos reikalavimus, yra atsakingas už tinkamą Saugos nuostatuose nustatytų funkcijų vykdymą;

13.7. atlieka kitas Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, Saugos nuostatuose, saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

14. Saugos įgaliotinis negali atlikti administratorių funkcijų.

15. Registro administratoriai pagal kompetenciją atlieka funkcijas, susijusias su Registro naudotojų administravimu, Registro komponentais (kompiuteriais, operacinėmis sistemomis, duomenų bazės valdymo sistemomis, taikomųjų programų sistemomis, ugniasienėmis, įsilaužimų aptikimo sistemomis, duomenų perdavimu tinklais, bylų serveriais ir kitais), šių Registro komponentų sąranka, Registro pažeidžiamų vietų nustatymu, saugos reikalavimų atitikties nustatymu ir stebėsena, reagavimu į Registro duomenų saugos incidentus ir jų valdymu, taip pat privalo vykdyti visus saugos įgaliotinio nurodymus ir pavedimus, susijusius su Registro saugos užtikrinimu, ir nuolat teikti saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę:

15.1. Registro naudotojų administratorius atlieka šias Registro naudotojų administravimo funkcijas:

15.1.1. registruoja ir išregistruoja Registro naudotojus;

15.1.2. suteikia, keičia ir panaikina Registro naudotojams prieigos prie Registro duomenų teises;

15.1.3. administruoja Registro naudotojų duomenis;

15.1.4. tvarko klasifikatorius;

15.1.5. analizuoja registracijos žurnalų įrašus;

15.1.6. atlieka kitas Registro valdytojo vadovo pavestas, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, Saugos

nuostatuose, saugos politiką įgyvendinančiuose ir kituose teisės aktuose nustatytas funkcijas, susijusias su Registro naudotojų teisių valdymu;

15.2. Registro kompiuterių tinklo administratorius atlieka šias funkcijas:

15.2.1. užtikrina kompiuterių tinklo veikimą;

15.2.2. projektuoja kompiuterių tinklus;

15.2.3. diegia, konfigūruoja ir prižiūri kompiuterių tinklų aktyviąją įrangą;

15.2.4. konfigūruoja Registro tarnybinių stočių (toliau – tarnybinės stotys) tinklo prieigą;

15.2.5. administruoja ugniasienes;

15.2.6. administruoja maršrutizatorius ir komutatorius;

15.2.7. administruoja pagalbinę įrangą (UPS, fizines linijas ir pan.);

15.2.8. užtikrina kompiuterių tinklo saugumą (nustato pažeidžiamas vietas);

15.2.9. atlieka kitas Registro valdytojo vadovo pavestas, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, Saugos nuostatuose, saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose nustatytas funkcijas, siekdamas užtikrinti tinkamą kompiuterių tinklo veikimą;

15.3. Registro tarnybinių stočių administratorius atlieka šias funkcijas:

15.3.1. užtikrina tarnybinių stočių veikimą;

15.3.2. konfigūruoja tarnybinių stočių tinklo prieigą;

15.3.3. kuria ir administruoja tarnybinių stočių naudotojų registracijos į tarnybines stotis duomenis;

15.3.4. stebi ir analizuoja tarnybinių stočių veiklą;

15.3.5. diegia ir konfigūruoja tarnybinių stočių programinę įrangą;

15.3.6. diegia tarnybinių stočių programinės įrangos naujinius ir pataisas, laikydamasis Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir informacinių sistemų pokyčių valdymo tvarkos aprašo, patvirtinto Lietuvos Respublikos vidaus reikalų ministro 2017 m. lapkričio 10 d. įsakymu Nr.1V-773 „Dėl Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir informacinių sistemų pokyčių valdymo tvarkos aprašo patvirtinimo“, (toliau − Registro pokyčių valdymo tvarkos aprašas);

15.3.7. užtikrina tarnybinių stočių saugą;

15.3.8. atlieka kitas Registro valdytojo vadovo pavestas, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, Saugos nuostatuose, saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose nustatytas funkcijas;

15.4. Registro duomenų bazės administratorius atlieka šias funkcijas:

15.4.1. užtikrina Registro duomenų bazės ir duomenų bazės archyvo, Registro duomenų atsarginio kopijavimo įrangos veikimą;

15.4.2. tvarko Registro programinę įrangą ir Registro duomenų bazės valdymo sistemos programinę įrangą;

15.4.3. diegia Registro programinės įrangos ir Registro duomenų bazės valdymo sistemos programinės įrangos naujinius ir pataisas, laikydamasis Registro pokyčių valdymo tvarkos aprašo;

15.4.4. atsako už Registro duomenų atsarginių kopijų darymą, saugojimą ir Registro duomenų iš atsarginių kopijų atkūrimą;

15.4.5. užtikrina Registro duomenų bazės ir duomenų bazės archyvo, Registro duomenų atsarginių kopijų saugą;

15.4.6. atlieka kitas Registro valdytojo vadovo pavestas, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, Saugos nuostatuose, saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose nustatytas funkcijas, susijusias su Registro duomenų bazės ir duomenų bazės archyvo, Registro duomenų atsarginių kopijų administravimu ir priežiūra.

16. Registro administratoriai pagal kompetenciją:

16.1. reaguoja į saugos incidentus ir juos valdo, atlieka įsilaužimų į Registrą aptikimo funkcijas;

16.2. dalyvauja atliekant informacinių sistemų rizikos vertinimą ir informacinių sistemų informacinių technologijų atitikties saugos reikalavimams vertinimą;

16.3. nuolat atnaujina Registro sąrankos aprašus, kad būtų rodoma esama Registro sąrankos būklė.

17. Registro administratoriai pagal kompetenciją yra atsakingi už tinkamą Registro saugos dokumentuose nustatytų funkcijų vykdymą.

18. Registro administratoriai privalo vykdyti visus saugos įgaliotinio nurodymus ir pavedimus, kad užtikrintų Registro duomenų saugą, pagal kompetenciją reaguoti į saugos incidentus, juos valdyti ir nuolat teikti saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę.

19. Teisės aktai, kuriais vadovaujantis tvarkomi Registro duomenys ir užtikrinama jų sauga:

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. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

19.3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

19.4. Lietuvos Respublikos kibernetinio saugumo įstatymas;

19.5. Lietuvos Respublikos įtariamųjų, kaltinamųjų ir nuteistųjų registro įstatymas;

19.6. Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas;

19.7. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

19.8. Kibernetinio saugumo reikalavimų aprašas;

19.9. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašas, patvirtintas Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

19.10. Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos informacijos saugos valdymo sistemos nuostatai, patvirtinti Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2019 m. balandžio 3 d. įsakymu Nr. 5V-35 „Dėl Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos informacijos saugos valdymo sistemos organizavimo“;

19.11. Kibernetinių incidentų valdymo Informatikos ir ryšių departamento prie Vidaus reikalų ministerijos valdomoje ypatingos svarbos informacinėje infrastruktūroje planas, patvirtintas Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus įsakymu „Dėl Kibernetinių incidentų valdymo Informatikos ir ryšių departamento prie Vidaus reikalų ministerijos valdomoje ypatingos svarbos informacinėje infrastruktūroje plano patvirtinimo ir Techninių kibernetinio saugumo reikalavimų įgyvendinimo Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos valdomoje ypatingos svarbos informacinėje infrastruktūroje“, (toliau − Kibernetinių incidentų valdymo planas);

19.12. Vidaus reikalų informacinės sistemos techninės ir programinės įrangos gedimo, sutrikimo ir kitų incidentų valdymo tvarkos aprašas, patvirtintas Lietuvos Respublikos vidaus reikalų ministro 2008 m. rugsėjo 10 d. įsakymu Nr. 1V-335 „Dėl Vidaus reikalų informacinės sistemos techninės ir programinės įrangos gedimo, sutrikimo ar kitų incidentų valdymo tvarkos aprašo patvirtinimo“;

19.13. Registro nuostatai;

19.14. Lietuvos standartai LST EN ISO/IEC 27002 ir LST EN ISO/IEC 27001 bei Lietuvos ir tarptautiniai „Informacinės technologijos. Saugumo metodai“ grupės standartai, reglamentuojantys saugų duomenų tvarkymą;

19.15. kiti teisės aktai, reglamentuojantys Registro duomenų tvarkymo teisėtumą, Registro valdytojo ir Registro tvarkytojo veiklą ir Registro duomenų saugos valdymą.

II SKYRIUS
REGISTRO DUOMENŲ SAUGOS VALDYMAS

20. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, (toliau – Klasifikavimo gairių aprašas) 7.2 ir 7.5 papunkčiais, Registre tvarkoma elektroninė informacija priskiriama ypatingos svarbos informacijos kategorijai.

21. Registras priskiriamas pirmajai kategorijai, vadovaujantis Klasifikavimo gairių aprašo 12.1 papunkčio nuostatomis ir atsižvelgiant į Registre apdorojamos elektroninės informacijos svarbos kategoriją.

22. Saugos įgaliotinis, vadovaudamasis Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos informacijos saugos rizikos vertinimo metodika, patvirtinta Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2019 m. balandžio 5 d. įsakymu Nr. 5V-37 „Dėl Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos informacijos saugos valdymo sistemos procedūrų patvirtinimo“, Lietuvos Respublikos vidaus reikalų ministerijos metodine priemone „Rizikos analizės vadovas“, Lietuvos ir tarptautiniais „Informacinės technologijos. Saugumo metodai“ grupės standartais, kartu su Informatikos ir ryšių departamento Teistumo informacijos tvarkymo skyriumi kasmet organizuoja Registro rizikos vertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį Registro rizikos vertinimą. Registro valdytojo rašytiniu pavedimu Registro rizikos vertinimą gali atlikti pats saugos įgaliotinis arba Registro rizikos veiksnių vertinimui atlikti gali būti perkamos rizikos vertinimo paslaugos.

23. Registro rizikos veiksniams vertinti naudojama Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistema (toliau – ARSIS).

24. Registro rizikos vertinimo rezultatai išdėstomi rizikos vertinimo ataskaitoje. Rizikos vertinimo ataskaita rengiama įvertinant rizikos veiksnius, galinčius turėti įtakos Registro duomenų saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausieji rizikos veiksniai yra šie:

24.1. subjektyvūs netyčiniai (Registro duomenų tvarkymo klaidos ir apsirikimai, Registro duomenų ištrynimas, klaidingas Registro duomenų teikimas, fiziniai informacinių technologijų sutrikimai, Registro duomenų perdavimo tinklais sutrikimai, Registro programinės įrangos klaidos, netinkamas veikimas ir kita);

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

24.3. 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.

25. Registro valdytojas, atsižvelgdamas į rizikos vertinimo ataskaitą, prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

26. Registro saugos priemonės parenkamos įvertinus galimus rizikos, kylančios Registro duomenų vientisumui, konfidencialumui ir prieinamumui, veiksnius.

27. Registro duomenų saugos būklė gerinama techninėmis, programinėmis, organizacinėmis ir kitomis duomenų saugos priemonėmis, kurios pasirenkamos atsižvelgiant į Registro valdytojo skiriamus išteklius ir vadovaujantis šiais principais:

27.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

27.2. Registro duomenų saugos priemonės diegimo kainos atitiktis saugomų Registro duomenų vertei;

27.3. esant galimybei, turi būti įdiegtos prevencinės korekcinės Registro duomenų saugos priemonės.

28. Siekiant užtikrinti Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, vadovaujantis Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos

patvirtinimo“, kasmet organizuojamas Registro informacinių technologijų saugos atitikties vertinimas.

29. Registro informacinių technologijų saugos atitikties vertinimo metu gali būti atliekamas pažeidžiamumų testavimas, imituojant kibernetines atakas ir vykdant kibernetinių incidentų imitavimo pratybas. Imituojant kibernetines atakas, rekomenduojama vadovautis tarptautiniu mastu pripažintų organizacijų (pvz.: *EC-COUNCIL, ISACA, NIST* ir kt.) rekomendacijomis ir gerąja praktika.

30. Registro informacinių technologijų saugos atitikties vertinimą ne rečiau kaip kartą per trejus metus turi atlikti nepriklausomi, visuotinai pripažintų tarptautinių organizacijų sertifikuoti valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų auditoriai.

31. Atlikus Registro informacinių technologijų saugos atitikties vertinimą, rengiamas nustatytų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nurodo Registro valdytojas.

32. Registro rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano, Registro informacinių technologijų saugos atitikties vertinimo ataskaitos ir nustatytų trūkumų šalinimo plano kopijas Registro valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia ARSIS Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatuose, patvirtintuose 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“, nustatyta tvarka.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

33. Registro programinės įrangos, skirtos Registrui apsaugoti nuo kenksmingosios programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir panašiai), naudojimo nuostatos ir jos atnaujinimo reikalavimai:

33.1. tarnybinėse stotyse ir Registro naudotojų kompiuterizuotose darbo vietose turi būti naudojamos centralizuotai valdomos kenksmingosios programinės įrangos aptikimo priemonės, kurios nuolat ieško ir blokuoja kenksmingąją programinę įrangą ir kurios turi būti reguliariai atnaujinamos automatiniu būdu ne rečiau kaip kartą per 24 valandas;

33.2. Registro programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

34. Registro programinės įrangos, įdiegtos tarnybinėse stotyse ir Registro naudotojų kompiuterizuotose darbo vietose, naudojimo nuostatos:

34.1. Registro darbui turi būti naudojama tik legali ir patikrinta programinė įranga, įtraukta į Kompiuterizuotose darbo vietose, kurias prižiūri Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos, leistinos programinės įrangos sąrašą, patvirtintą Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2006 m. gruodžio 29 d. įsakymu Nr. 5V-91 „Dėl Kompiuterizuotų darbo vietų priežiūros paslaugų teikimo taisyklių patvirtinimo“. Leistinos programinės įrangos sąrašą pagal poreikį peržiūri ir prireikus atnaujina saugos įgaliotinis kartu su Informatikos ir ryšių departamento Informacinių technologijų paslaugų skyriumi, Registro duomenų bazės ir Registro tarnybinių stočių administratoriais;

34.2. Registro programinė įranga prižiūrima ir nuolat atnaujinama laikantis gamintojo rekomendacijų;

34.3. Registro programinės įrangos diegimą, šalinimą ir konfigūravimą pagal kompetenciją atlieka tik Registro duomenų bazės arba Registro tarnybinių stočių administratorius.

35. Turi būti naudojamos tik tarnybinės išorinės duomenų laikmenos (USB, CD / DVD ir kt.) bei kiti tarnybiniai įrenginiai, kurie yra išduoti tarnybinėms funkcijoms vykdyti.

36. Registro naudotojų kompiuterizuotose darbo vietose turi būti įdiegtos priemonės, leidžiančios riboti išorinių duomenų laikmenų (USB, CD / DVD ir kt.) naudojimą.

37. Registro programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims.

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

38.1. Registrui naudojamas Vidaus reikalų telekomunikacinis tinklas (toliau – VRTT), už kurio administravimą ir priežiūrą atsako šio tinklo pagrindinis tvarkytojas, turi būti atskirtas nuo kitų tinklų ugniasienėmis, DOS ir DDOS atakų prevencijai skirta įranga bei įsilaužimų aptikimo ir prevencijos įranga;

38.2. visas duomenų srautas į internetą ir iš jo turi būti filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingosios programinės įrangos;

38.3. turi būti naudojamos turinio filtravimo sistemos;

38.4. turi būti naudojamos taikomųjų programų kontrolės sistemos.

39. Metodai, kuriais leidžiama užtikrinti saugų Registro duomenų teikimą ir (ar) gavimą:

39.1. Registro naudotojų, jų vykdytų užklausų ir peržiūrėtų užklausų rezultatų duomenys tvarkomi naudotojų administravimo posistemėje Vidaus reikalų informacinės sistemos centrinio

duomenų banko duomenų peržiūros kontrolės taisyklėse, patvirtintose Lietuvos Respublikos vidaus reikalų ministro 2005 m. kovo 9 d. įsakymu Nr. 1V-68 „Dėl Vidaus reikalų informacinės sistemos centrinio duomenų banko duomenų peržiūros kontrolės taisyklių patvirtinimo“, nustatyta tvarka;

39.2. tiesioginė prieiga prie Registro duomenų suteikiama įgyvendinus Registro naudotojų autentifikavimo priemones – Registro naudotojai tapatybę patvirtina slaptažodžiu. Registro naudotojų slaptažodžiai sudaromi, keičiami ir jų galiojimo trukmė nustatoma, vadovaujantis Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų naudotojų administravimo taisyklėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2018 m. lapkričio 26 d. įsakymu Nr. 1V-871, (toliau – Naudotojų administravimo taisyklės). Tiesioginė prieiga prie Registro duomenų užtikrinama automatiniu būdu visą parą, darbo ir poilsio dienomis;

39.3. prieiga prie Registro suteikiama tik registruotiems Registro naudotojams;

39.4. Registro duomenys perduodami automatiniu būdu naudojant TCP / IP, HTTPS protokolus realiu laiku (tiesioginiu režimu (angl. *online*)) arba asinchroniniu režimu pagal duomenų teikimo sutartis, kuriose nustatytos perduodamų duomenų specifikacijos, kopijų skaičius, kitos duomenų perdavimo sąlygos ir tvarka;

39.5. Registro duomenys, perduodami per VRTT ir kitas duomenų perdavimo linijas, turi būti šifruojami.

40. Registro duomenims perduoti naudojamas VRTT ir kiti saugūs elektroninių ryšių tinklai.

41. Visos Registro naudotojų kompiuterizuotos darbo vietos turi būti valdomos naudojant centralizuoto valdymo priemones (pvz., katalogų tarnybą „*Active direktory*“).

42. Registro naudotojų tarnybinėms funkcijoms vykdyti naudojamuose nešiojamuose kompiuteriuose turi būti naudojamas kompiuterio įjungimo slaptažodis, papildomas Registro naudotojo tapatybės patvirtinimas ir elektroninės informacijos šifravimas.

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

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

43.2. prie Registro prisijungiama nuotoliniu būdu naudojant interneto naršyklę (HTTPS protokolą).

44. Registro atsarginių duomenų kopijų darymo ir atkūrimo reikalavimai nustatyti Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos administruojamų informacinių sistemų ir registrų elektroninės informacijos atsarginių kopijų darymo, saugojimo ir atkūrimo tvarkos apraše, patvirtintame Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2017 m. sausio 9 d. įsakymu Nr. 5V-6 „Dėl Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos administruojamų informacinių sistemų ir registrų elektroninės informacijos atsarginių kopijų darymo, saugojimo ir atkūrimo tvarkos aprašo patvirtinimo“.

45. Turi būti užtikrintas saugos incidentų, įvykusių Registre, registravimas, valdymas ir tyrimas Kibernetinių saugumo reikalavimų apraše, Kibernetinių incidentų valdymo plane ir Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų veiklos tęstinumo valdymo plane, patvirtintame Lietuvos Respublikos vidaus reikalų ministro 2018 m. lapkričio 26 d. įsakymu Nr. 1V-871 „Dėl Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklių, naudotojų administravimo taisyklių ir veiklos tęstinumo valdymo plano patvirtinimo“, nustatyta tvarka:

45.1. registruojami Registre įvykę saugos incidentai ir nedelsiant į juos reaguojama, techninėmis ir programinėmis priemonėmis saugos incidentai valdomi, tiriami, šalinami ir atkuriama Registro veikla;

45.2. Nacionaliniam kibernetinio saugumo centrui ir kitoms atsakingoms institucijoms pagal kompetenciją pranešama apie įvykusius saugos incidentus, jų vertinimą ir suvaldymą.

46. Ne rečiau kaip kartą per savaitę turi būti atliekama Registro naudotojų veiksmų audito įrašų analizė.

47. Ne rečiau kaip kartą per mėnesį turi būti atliekama ugniasienių užfiksuotų įvykių analizė ir nustatytos neatitiktys saugumo reikalavimams nedelsiant šalinamos.

48. Ne rečiau kaip kartą per mėnesį turi būti įvertinami kibernetiniam saugumui užtikrinti naudojamų priemonių programiniai atnaujinimai, klaidų taisymai ir šie atnaujinimai diegiami.

49. Perkant paslaugas, darbus ar įrangą, susijusius su Registru, jo projektavimu, kūrimu, diegimu, modernizavimu, priežiūra, palaikymu, saugos užtikrinimu, auditavimu, patalpų priežiūra, elektroninės informacijos perdavimo tinklais, įskaitant, bet neapsiribojant suteikiančius teisę ir galimybę prieiti prie Registro duomenų, juos apdoroti, saugoti, keistis duomenimis ar tiekti informacinių technologijų infrastruktūros komponentus, pirkimo dokumentuose iš anksto turi būti nustatyta, kad paslaugų teikėjas, darbų vykdytojas ar techninės ir programinės įrangos tiekėjas (toliau – paslaugų teikėjas) privalo laikytis Registro saugos dokumentuose nustatytų reikalavimų ir

užtikrinti teikiamų paslaugų, vykdomų darbų ar tiekiamos įrangos atitiktį nustatytiems elektroninės informacijos saugos reikalavimams.

50. Į paslaugų pirkimo sutartį turi būti įtraukta nuostata, įpareigojanti paslaugų teikėjo darbuotojus pasirašyti konfidencialumo pasižadėjimą neatskleisti tretiesiems asmenims jokios informacijos, gautos vykdant šią sutartį, išskyrus tą informaciją, kuri būtina sutarčiai vykdyti, taip pat nenaudoti konfidencialios informacijos asmeniniams ar trečiųjų asmenų poreikiams laikantis principo, kad visa paslaugų teikėjui suteikta informacija (įskaitant Registre tvarkomus duomenis) yra konfidenciali, nebent raštu patvirtinama, kad tam tikra pateikta informacija nėra konfidenciali.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

51. Saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą, tobulinti kvalifikaciją elektroninės informacijos saugos srityje.

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

53. Registro administratoriai privalo išmanyti pagrindinius elektroninės informacijos saugos ir saugaus darbo su duomenų perdavimo tinklais principus, atsižvelgiant į vykdomas funkcijas, atitinkamai turėti sisteminių programinių priemonių administravimo ir priežiūros patirties, mokėti administruoti ir prižiūrėti Registro duomenų bazę, 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, turėti sisteminių programinių priemonių (*Windows, Unix, Oracle*) administravimo ir priežiūros patirties.

54. Registro administratoriai ir Registro naudotojai turi būti susipažinę su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais, pagal kompetenciją ir kitais teisės aktais bei standartais, reglamentuojančiais elektroninės informacijos saugą.

55. Registro naudotojai, atliekantys tarnybines funkcijas, susijusias su asmens duomenų tvarkymu bei teikimu, pasirašytinai supažindinami su asmens duomenų tvarkymą ir saugą reglamentuojančiais teisės aktais ir atsakomybe už jų pažeidimą ir raštu įpareigojami saugoti asmens duomenų paslaptį. Asmens duomenų paslaptį jie privalo saugoti ir pradėję eiti kitas pareigas, pasibaigus jų darbo (tarnybos) ar sutartiniams santykiams.

56. Registro naudotojai, pastebėję saugos dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai Informatikos ir ryšių departamento Informacinių ir telekomunikacinių technologijų pagalbos grupei (toliau – ITT pagalbos grupė) arba administratoriams, arba saugos įgaliotiniui.

57. Visi Registro naudotojai privalo:

57.1. turėti pagrindinių darbo kompiuteriu, taikomosiomis programomis įgūdžių, mokėti saugiai tvarkyti Registro duomenis;

57.2. nuolat kelti kvalifikaciją saugaus elektroninės informacijos tvarkymo kursuose, mokymuose, seminaruose;

57.3. įtarę, kad prisijungimo prie Registro slaptažodis galėjo būti atskleistas kitam asmeniui, praradę ar kitaip netekę slaptažodžio, nedelsdami informuoti ITT pagalbos grupę; nurodytais atvejais slaptažodis turi būti pakeistas Naudotojų administravimo taisyklėse nustatyta tvarka.

58. Registro naudotojams draudžiama:

58.1. atskleisti Registro duomenis ar suteikti kitokią galimybę bet kokia forma su jais susipažinti tokios teisės neturintiems asmenims;

58.2. savavališkai diegti Registro taikomosios programinės įrangos pakeitimus ir naujas versijas neturint tam suteiktos teisės;

58.3. atskleisti kitiems asmenims prisijungimo prie Registro vardą, slaptažodį ar kitaip sudaryti sąlygas jais pasinaudoti;

58.4. naudoti Registro duomenis kitokiais nei Registro nuostatuose nurodytais tikslais bei savo pareigybės aprašyme nustatytų funkcijų vykdymo tikslais;

58.5. sudaryti sąlygas pasinaudoti Registrui tvarkyti naudojama technine ir programine įranga tokios teisės neturintiems asmenims (paliekant darbo vietą būtina užrakinti darbalaukį arba išjungti darbo stotį);

58.6. atlikti veiksmus, dėl kurių gali būti neteisėtai pakeisti, sunaikinti ar atskleisti Registro duomenys, taip pat neatlikti būtinų veiksmų, kurie apsaugo Registro duomenis;

58.7. savavališkai prijungti prie Registro naudotojų kompiuterizuotų darbo vietų išorines duomenų laikmenas ar įrenginius, išskyrus nurodytus Saugos nuostatų 35 punkte;

58.8. atlikti bet kokius kitus neteisėtus Registro tvarkymo veiksmus.

59. Registro naudotojams turi būti rengiami duomenų saugos mokymai, įvairiais būdais primenama apie saugos problematiką (pvz.: priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės ir pan.). Saugos mokymai organizuojami kartą per metus, mokymus organizuoja saugos įgaliotinis arba duomenų apsaugos pareigūnas pagal kompetenciją.

V SKYRIUS
REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

60. Tvarkyti Registro duomenis gali tik Registro naudotojai, susipažinę su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant Registro duomenis, užtikrinant jų saugą, taip pat su atsakomybe už saugos dokumentų nuostatų pažeidimus, ir sutikę laikytis saugos dokumentuose nustatytų reikalavimų. Pakartotinis supažindinimas vykdomas pasikeitus minėtiems dokumentams ir teisės aktams.

61. Registro naudotojų supažindinimą su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais organizuoja saugos įgaliotinis.

62. Registro naudotojai su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais bei atsakomybe už jų reikalavimų nesilaikymą supažindinami pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodomumą (jungiantis prie DVS, Registro per naudotojo sąsają ar pan.).

63. Saugos nuostatai ir saugos politiką įgyvendinantys dokumentai turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per kalendorinius metus. Saugos dokumentai turi būti persvarstomi (peržiūrimi) atlikus rizikos veiksnių analizę ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams. Saugos įgaliotinis pagal kompetenciją atsakingas, kad Registro naudotojai būtų informuoti apie jų pakeitimą ir (ar) pripažinimą netekusiais galios.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

64. Patvirtinęs Saugos nuostatus ar jų pakeitimus, Registro valdytojas Registrų ir valstybės informacinių sistemų registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės

2012 m. spalio 16 d. nutarimu Nr. 1263 „Dėl Registrų sąrašo reorganizavimo į Registrų ir valstybės informacinių sistemų registrą ir Registrų ir valstybės informacinių sistemų registro nuostatų patvirtinimo“, nustatyta tvarka pateikia šiam registrui reikalingus duomenis ar dokumentų kopijas.

65. Patvirtintų saugos politiką įgyvendinančių dokumentų ir jų pakeitimų kopijas Registro valdytojas ne vėliau kaip per 5 darbo dienas nuo jų patvirtinimo turi pateikti ARSIS Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatuose, patvirtintuose Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V- 1183, nustatyta tvarka.

Pakeitimai:

1.
Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos, Įsakymas
Nr. 5V-49, 2015-09-24, paskelbta TAR 2015-09-24, i. k. 2015-14176
Dėl Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2012 m. liepos 4 d. įsakymo Nr. 5V-57 „Dėl Įtariamųjų, kaltinamųjų ir nuteistųjų registro duomenų saugos nuostatų patvirtinimo“ pakeitimo

2.
Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos, Įsakymas
Nr. 5V-1, 2016-01-05, paskelbta TAR 2016-01-05, i. k. 2016-00079
Dėl Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2012 m. liepos 4 d. įsakymo Nr. 5V-57 „Dėl Įtariamųjų, kaltinamųjų ir nuteistųjų registro duomenų saugos nuostatų patvirtinimo“ pakeitimo

3.
Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos, Įsakymas
Nr. 5V-8, 2018-01-18, paskelbta TAR 2018-01-18, i. k. 2018-00805
Dėl Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2012 m. liepos 4 d. įsakymo Nr. 5V-57 „Dėl Įtariamųjų, kaltinamųjų ir nuteistųjų registro duomenų saugos nuostatų patvirtinimo“ pakeitimo

4.
Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos, Įsakymas
Nr. 5V-21, 2021-02-26, paskelbta TAR 2021-03-01, i. k. 2021-04022
Dėl Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2012 m. liepos 4 d. įsakymo Nr. 5V-57 „Dėl Įtariamųjų, kaltinamųjų ir nuteistųjų registro duomenų saugos nuostatų patvirtinimo“ pakeitimo