Įsakymas netenka galios 2021-08-03:

Priešgaisrinės apsaugos ir gelbėjimo departamentas prie Vidaus reikalų ministerijos, Įsakymas Nr. 1-456, 2021-08-02, paskelbta TAR 2021-08-02, i. k. 2021-16955

Dėl Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus 2016 m. sausio 4 d. įsakymo Nr. 1/2015-412 „Dėl Valstybinės reikšmės ir pavojingų objektų registro duomenų saugos nuostatų, Valstybinės reikšmės ir pavojingų objektų registro saugaus elektroninės informacijos tvarkymo taisyklių, Valstybinės reikšmės ir pavojingų objektų registro naudotojų administravimo taisyklių ir Valstybinės reikšmės ir pavojingų objektų registro veiklos tęstinumo valdymo plano patvirtinimo“ pripažinimo netekusiu galios

Suvestinė redakcija nuo 2019-11-16 iki 2021-08-02

Įsakymas paskelbtas: TAR 2016-01-04, i. k. 2016-00020

PRIEŠGAISRINĖS APSAUGOS IR GELBĖJIMO DEPARTAMENTO PRIE VIDAUS REIKALŲ MINISTERIJOS DIREKTORIUS

ĮSAKYMAS DĖL VALSTYBINĖS REIKŠMĖS IR PAVOJINGŲ OBJEKTŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ, VALSTYBINĖS REIKŠMĖS IR PAVOJINGŲ OBJEKTŲ REGISTRO SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLIŲ, VALSTYBINĖS REIKŠMĖS IR PAVOJINGŲ OBJEKTŲ REGISTRO NAUDOTOJŲ ADMINISTRAVIMO TAISYKLIŲ IR VALSTYBINĖS REIKŠMĖS IR PAVOJINGŲ OBJEKTŲ REGISTRO VEIKLOS TĘSTINUMO VALDYMO PLANO PATVIRTINIMO

2016 m. sausio 4 d. Nr. 1/2015-412
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 7 punktu:

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

1.1. *Neteko galios nuo 2019-10-05*

Punkto naikinimas:
Nr. 1-414, 2019-10-04, paskelbta TAR 2019-10-04, i. k. 2019-15863

1.2. Valstybinės reikšmės ir pavojingų objektų registro saugaus elektroninės informacijos tvarkymo taisykles;

1.3. Valstybinės reikšmės ir pavojingų objektų registro naudotojų administravimo taisykles;

1.4. Valstybinės reikšmės ir pavojingų objektų registro veiklos tęstinumo valdymo planą.

2. P r i p a ž į s t u netekusiu galios:

2.1. Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus 2007 m. birželio 29 d. įsakymą Nr. 1-207 „Dėl Valstybinės reikšmės ir pavojingų objektų registro duomenų saugos nuostatų patvirtinimo“ su visais pakeitimais ir papildymais;

2.2. Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus 2009 m. vasario 18 d. įsakymą Nr. 1-67 „Dėl Valstybinės reikšmės ir pavojingų objektų registro saugaus elektroninės informacijos tvarkymo taisyklių patvirtinimo“;

2.3. Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus 2008 m. gegužės 14 d. įsakymą Nr. 1-150 „Dėl Valstybinės reikšmės ir pavojingų objektų registro naudotojų administravimo taisyklių patvirtinimo“;

2.4. Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus 2008 m. sausio 17 d. įsakymą Nr. 1-12 „Dėl Valstybinės reikšmės ir pavojingų objektų registro veiklos tęstinumo valdymo plano patvirtinimo“.

3. *Neteko galios nuo 2019-10-05*

Punkto naikinimas:

Nr. 1-414, 2019-10-04, paskelbta TAR 2019-10-04, i. k. 2019-15863

4. *Neteko galios nuo 2019-11-16*

Punkto naikinimas:

Nr. 1-472, 2019-11-15, paskelbta TAR 2019-11-15, i. k. 2019-18335

Direktorius
vidaus tarnybos generolas Remigijus Baniulis

SUDERINTA
Lietuvos Respublikos
vidaus reikalų ministerijos
Viešojo valdymo politikos
departamento
2015 m. gruodžio 28 d.
raštu Nr. 31D-673

Patvirtinta. *Neteko galios nuo 2019-10-05*

Priedo naikinimas:

Nr. 1-414, 2019-10-04, paskelbta TAR 2019-10-04, i. k. 2019-15863

PATVIRTINTA
Priešgaisrinės apsaugos ir gelbėjimo
departamento prie Vidaus reikalų
ministerijos direktoriaus
2016 m. sausio 4 d.
įsakymu Nr. 1/2015-412

VALSTYBINĖS REIKŠMĖS IR PAVOJINGŲ OBJEKTŲ REGISTRO NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės reikšmės ir pavojingų objektų registro naudotojų administravimo taisyklės (toliau – Administravimo taisyklės) nustato Valstybinės reikšmės ir pavojingų objektų registro (toliau – Registras) naudotojų administravimo principus ir tvarką, jų teises, pareigas ir kontrolę.

2. Administravimo taisyklėse vartojamos sąvokos atitinka Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas), Valstybinės reikšmės ir pavojingų objektų registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2000 m. lapkričio 8 d. nutarimu Nr. 1386 „Dėl Pavojingų Lietuvos ūkio objektų registro reorganizavimo į Valstybinės reikšmės ir pavojingų objektų registrą“, Valstybinės reikšmės ir pavojingų objektų registro duomenų saugos nuostatuose, patvirtintuose Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos (toliau – PAGD) direktoriaus 2007 m. birželio 29 d. įsakymu Nr. 1-207 (toliau – Saugos nuostatai) ir kituose saugų elektroninės informacijos bei duomenų tvarkymą reglamentuojančiuose teisės aktuose apibrėžtas sąvokas.

3. Administravimo taisyklių reikalavimai taikomi visiems Registro naudotojams, administratoriams, saugos įgaliotiniui.

4. Už Administravimo taisyklių įgyvendinimo kontrolę atsakingas saugos įgaliotinis.

5. Registro naudotojai, administratoriai vadovaujasi prieigos prie elektroninės informacijos principu – viskas yra draudžiama, kas nėra leidžiama.

II SKYRIUS
REGISTRO NAUDOTOJŲ IR ADMINISTRATORIŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

6. Registro naudotojai naudojasi tik tais Registro posistemiais ir juose apdorojama elektronine informacija, prie kurių prieiga jiems yra numatyta pagal pareigas ir kurią suteikė administratorius.

7. Registro naudotojų įgaliojimai ir teisės:

7.1. peržiūrėti elektroninę informaciją;

7.2. reikalauti iš administratorių ir saugos įgaliotinio deramo jų naudojamų ir Registre apdorojamų duomenų saugos lygio užtikrinimo, gauti informaciją apie taikomas saugos priemones ir rekomenduoti papildomas saugos priemones.

8. Vidiniai Registro naudotojai kartu su išvardytais 7 punkte įgaliojimais ir teisėmis papildomai turi šiuos įgaliojimus ir teises:

8.1. įrašyti elektroninę informaciją;

8.2. redaguoti, keisti, atnaujinti elektroninę informaciją.

9. Registro naudotojų pareigos:

9.1. susipažinti su Saugos nuostatais, Valstybinės reikšmės ir pavojingų objektų registro saugaus elektroninės informacijos tvarkymo taisyklėmis, Valstybinės reikšmės ir pavojingų objektų registro veiklos tęstinumo valdymo planu ir Administravimo taisyklėmis (toliau – Registro saugos politiką įgyvendinantys dokumentai);

9.2. užtikrinti Registro tvarkomos elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą, vadovautis Saugos nuostatuose ir kituose Registro saugos politiką įgyvendinančiuose dokumentuose nustatytais reikalavimais;

9.3. saugoti prisijungimo prie Registro slaptažodžius ir kitą prisijungimo prie Registro informaciją, jos neplatinti ir užtikrinti tinkamą apsaugą nuo trečiųjų asmenų;

9.4. nedelsdamas pakeisti prisijungimo slaptažodį, jeigu įtaria, kad jo slaptažodį sužinojo kitas asmuo;

9.5. pastebėję Registro saugos politiką įgyvendinančiuose dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, Registro sutrikimus, neįprastą jo veikimą, nedelsdami praneša apie tai administratoriui, saugos įgaliotiniui arba PAGD informacinių technologijų pagalbos tarnybai (toliau – IT pagalbos tarnyba).

10. Administratoriai atlieka Saugos nuostatų 11 punkte nurodytas funkcijas. Administratorių įgaliojimai, teisės ir pareigos:

10.1. duomenų tvarkymo administratorių įgaliojimai ir teisės:

10.1.1. skaityti, kurti, atnaujinti, naikinti Registro duomenis;

10.1.2. atlikti Registro naudotojų administravimo veiksmus;

10.1.3. stebėti Registro naudotojų su Registro tvarkomais duomenimis atliktus veiksmus;

10.2. duomenų tvarkymo administratorių pareigos:

10.2.1. tinkamai ir laiku atlikti Registro naudojamų duomenų tvarkymą;

10.2.2. užtikrinti tinkamą Registro naudotojų administravimą ir jų veiksmų stebėjimą.

10.3. sisteminių administratorių įgaliojimai ir teisės:

10.3.1. administruoti Registrą sudarančius komponentus (kompiuterius, operacines sistemas, duomenų bazių valdymo sistemas, taikomųjų programų sistemas, užkardas, įsilaužimų aptikimo sistemas, elektroninės informacijos perdavimo tinklus, bylų serverius ir kt.);

10.3.2. fiziškai prieiti prie Registro techninės įrangos;

10.4. sisteminių administratorių pareigos:

10.4.1. atlikti tinkamą Registrą sudarančių komponentų administravimą;

10.4.2. pagal kompetenciją vykdyti Registro techninės įrangos priežiūros funkcijas;

10.4.3. pagal kompetenciją atlikti techninės įrangos remontą;

10.4.4. užtikrinti nepertraukiamą Registro techninės ir sisteminės programinės įrangos veikimą.

11. Administratoriai pagal kompetenciją diegia ir įgyvendina Registro duomenų saugos priemones.

12. Atlikdami Registro sąrankos pakeitimus, administratoriai laikosi PAGD nustatytos Registro pokyčių valdymo tvarkos, nustatytos Valstybinės reikšmės ir pavojingų objektų registro saugaus elektroninės informacijos tvarkymo taisyklėse. Kartą per metus arba po Registro pokyčio patikrina (peržiūri) Registro sąranką ir Registro būsenos rodiklius.

13. Sisteminių administratorių ir duomenų tvarkymo administratorių veiklą koordinuoja jų tiesioginiai vadovai.

III SKYRIUS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO REGISTRO NAUDOTOJAMS KONTROLĖS TVARKA

14. Saugos įgaliotinis organizuoja Registro naudotojų supažindinimą su reikalavimais, išdėstytais Saugos dokumentuose.

15. Registro naudotojai supažindinami su Saugos dokumentais šiais atvejais:

15.1. prieš suteikiant Registro naudotojui prieigą prie Registro;

15.2. pakeitus Saugos dokumentus;

15.3. periodiškai, informacijos saugos mokymų metu, ne rečiau kaip kartą per metus.

16. Registro naudotojai supažindinami su Saugos dokumentais per PAGD nuotolinių mokymų tinklalapį.

17. Saugos įgaliotinis savo nuožiūra gali taikyti kitas supažindinimo formas (surengia trumpą seminarą, informuoja elektroniniu paštu ir (ar) per IT pagalbos tarnybos tinklalapį.

18. Saugos įgaliotinis tvarko Registro naudotojų susipažinimo su Saugos dokumentais elektroninį žurnalą.

19. Už Registro naudotojų registravimo ir išregistravimo, prieigos prie Registro teisių suteikimo, pakeitimo, sustabdymo, panaikinimo, unikalių prisijungimo prie Registro vardų ir pirminių prisijungimo slaptažodžių perdavimą Registro naudotojams atsakingi duomenų tvarkymo administratoriai.

20. Prisijungimo prie Registro teisės būsimiems Registro naudotojams suteikiamos tokia tvarka:

20.1. vidinio Registro naudotojo tiesioginis vadovas, Registro duomenų gavėjo atsakingas asmuo, kuris nurodytas duomenų teikimo sutartyje (toliau – atsakingas asmuo), IT pagalbos tarnybos elektroniniu paštu pateikia duomenų tvarkymo administratoriui būsimojo Registro naudotojo užpildytą prašymą „Dėl Registro naudotojo teisių suteikimo (pakeitimo, sustabdymo, panaikinimo)“ (toliau – prašymas);

20.2. duomenų tvarkymo administratorius per vieną darbo dieną nuo prašymo gavimo elektroniniu paštu pateikia Registro naudotojui prisijungimo prie PAGD nuotolinių mokymų tinklalapio įvadinę instrukciją, prisijungimo prie PAGD nuotolinių mokymų tinklalapio identifikatorių ir slaptažodį, informaciją, kaip susipažinti su Saugos dokumentais, Registro naudotojo įvadinę instrukciją, administratoriaus ir saugos įgaliotinio elektroninio pašto adresus ir telefonų numerius. Duomenų tvarkymo administratorius informuoja saugos įgaliotinį apie poreikį įregistruoti būsimą Registro naudotoją;

20.3. būsimasis Registro naudotojas, susipažįsta su Registro nuostatais ir Registro saugą įgyvendinančiais dokumentais ir išlaiko žinių patikrinimo testą. Išlaikęs testą, būsimas Registro naudotojas pasirašo Administravimo taisyklių priede pateiktą pasižadėjimą laikytis duomenų saugos reikalavimų tvarkant Registro elektroninę informaciją (toliau – pasižadėjimas). Pasirašytas pasižadėjimas pateikiamas IT pagalbos tarnybos elektroniniu paštu;

20.4. saugos įgaliotinis, įsitikinęs, kad būsimasis Registro naudotojas įvykdė 20.3. papunkčio reikalavimus, per vieną darbo dieną prašymą vizuoja ir perduoda duomenų tvarkymo administratoriui;

20.5. gavęs saugos įgaliotinio vizuotą prašymą, duomenų tvarkymo administratorius per vieną darbo dieną elektroniniu paštu pateikia Registro naudotojui prisijungimo prie Registro užšifruotą pirminį slaptažodį. Prisijungimo prie Registro identifikatorius ir informacija, kaip iššifruoti pirminį prisijungimo slaptažodį, pateikiama, esant techninėms galimybėms, šifruotu kanalu ar saugiu elektroninių ryšių tinklu, SMS (angl. *Short message service*) žinute, balsu. Duomenų tvarkymo administratorius pasirašo ant prašymo ir perduoda prašymą saugoti.

21. Prieigos prie Registro teisės Registro naudotojams keičiamos, sustabdomos, panaikinamos tokia tvarka:

21.1. vidinio Registro naudotojo tiesioginis vadovas, atsakingas asmuo IT pagalbos tarnybos elektroniniu paštu pateikia duomenų tvarkymo administratoriui Registro naudotojo užpildytą prašymą;

21.2. duomenų tvarkymo administratorius per vieną darbo dieną pakeičia, sustabdo, panaikina Registro naudotojo teisę dirbti su konkrečia elektronine informacija ir elektroniniu paštu informuoja apie tai Registro naudotoją. Duomenų tvarkymo administratorius pasirašo ant prašymo ir perduoda prašymą saugoti.

22. Registro naudotojų prieigos teisės keičiamos, sustabdomos šiais atvejais:

22.1. pasikeitus einamosioms pareigoms;

22.2. kai įstatymų nustatytais atvejais Registro naudotojas nušalinamas nuo darbo (pareigų);

22.3. kai vidinis Registro naudotojas nesinaudoja Registru ilgiau kaip 3 mėnesius;

22.4. pasibaigus tarnybos (darbo) santykiams;

22.5. esant kitoms aplinkybėms, dėl kurių būtina riboti naudotojo prieigą prie Registro.

23. Administratorius sustabdo prieigos prie Registro teisę, jeigu kyla pagrįstų įtarimų arba pateikiama informacija, kad Registro naudotojas piktnaudžiauja suteiktomis prieigos teisėmis ir gali pažeisti Registro ir jo apdorojamos elektroninės informacijos saugą. Administratorius praneša apie tokius veiksmus saugos įgaliotiniui.

24. Duomenų tvarkymo administratorius tvarko Registro naudotojų teisių suteikimo, pakeitimo, sustabdymo arba panaikinimo elektroninį žurnalą.

25. Pasižadėjimai ir prašymai saugojami PAGD dokumentacijos plano numatyta tvarka.

26. Registro naudotojų ir administratorių tapatybė Registre nustatoma pagal unikalų naudotojo prisijungimo vardą (identifikatorių) ir slaptažodį.

27. Slaptažodžių sudarymo, galiojimo trukmės ir keitimo reikalavimai yra šie:

27.1. slaptažodis sudarytas iš raidžių, skaičių ir specialiųjų simbolių;

27.2. slaptažodžiui sudaryti draudžiama naudoti asmeninio pobūdžio informaciją;

27.3. draudžiama slaptažodį atskleisti tretiesiems asmenims;

27.4. Registro posistemiai, atliekantys nutolusio prisijungimo autentifikavimą, draudžia automatiškai išsaugoti slaptažodžius;

27.5. didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius Registre yra ne didesnis nei 5 mėginimai. Neteisingai įvedus slaptažodį daugiau nei 5 kartus, Registras užsirakina ir 15 minučių neleidžia Registro naudotojui identifikuotis pakartotinai;

27.6. draudžiama slaptažodžius saugoti ar perduoti atviru tekstu ar užšifruoti nepatikimais algoritmais. Saugos įgaliotinio sprendimu tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jei Registro naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio arba nėra techninių galimybių Registro naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu.

28. Papildomi reikalavimai Registro naudotojų slaptažodžiams:

28.1. slaptažodis sudaromas iš ne mažiau kaip 8 simbolių;

28.2. slaptažodis keičiamas ne rečiau kaip kas 3 mėnesius. Keičiant slaptažodį Registras neleidžia nustatyti slaptažodžio iš buvusių 6 paskutinių slaptažodžių;

28.3. pirmojo prisijungimo prie Registro metu iš Registro naudotojo reikalaujama, kad jis pakeistų pirminį slaptažodį.

29. Papildomi reikalavimai administratorių slaptažodžiams:

29.1. slaptažodis sudaromas iš ne mažiau kaip 12 simbolių;

29.2. slaptažodis keičiamas ne rečiau kaip kas 2 mėnesius;

29.3. keičiant slaptažodį Registras neleidžia sudaryti slaptažodžio iš buvusių 3 paskutinių slaptažodžių.

30. Registro naudotojas, įtaręs, kad tretieji asmenys žino jo slaptažodį, nedelsdamas jį pakeičia. Jei pakeisti slaptažodžio nepavyko, Registro naudotojas pamiršo ar kitaip prarado slaptažodį, Registro naudotojas IT pagalbos tarnybos elektroniniu paštu informuoja duomenų

tvarkymo administratorių apie poreikį pakeisti arba atkurti slaptažodį. Duomenų tvarkymo administratorius per vieną darbo dieną elektroniniu paštu pateikia Registro naudotojui prisijungimo prie Registro užšifruotą pirminį slaptažodį. Prisijungimo prie Registro identifikatorius ir informacija, kaip iššifruoti pirminį prisijungimo slaptažodį, pateikiama, esant techninėms galimybėms, šifruotu kanalu ar saugiu elektroninių ryšių tinklu, SMS žinute, balsu.

31. Registro naudotojams, kuriems būtinas prisijungimas prie Registro iš nutolusios darbo vietos, yra taikomi Saugos nuostatų 26, 27.3 ir 27.5.2 papunkčių reikalavimai.

32. Vidiniai Registro naudotojai prie Registro prisijungti gali tik naudodamiesi kompiuterizuotomis darbo vietomis, įjungtomis į VRM telekomunikacijų tinklą.

IV SKYRIUS
BAIGIAMOSIOS NUOSTATOS

33. Saugos įgaliotinis, administratoriai, Registro naudotojai už Administravimo taisyklių pažeidimus atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

34. Kaip laikomasi Administravimo taisyklių, tikrinama atliekant Registro saugos atitikties vertinimą arba neplanuotą patikrinimą.

_____

Valstybinės reikšmės ir pavojingų objektų registro naudotojų administravimo taisyklių priedas

(Pasižadėjimo laikytis Valstybinės reikšmės ir pavojingų objektų registro duomenų saugos nuostatų ir kitų saugos politiką įgyvendinančių dokumentų reikalavimų forma)

PASIŽADĖJIMAS
LAIKYTIS VALSTYBINĖS REIKŠMĖS IR PAVOJINGŲ OBJEKTŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ IR KITŲ SAUGOS POLITIKĄ ĮGYVENDINANČIŲ DOKUMENTŲ REIKALAVIMŲ

_____ Nr. _____
(data) (registracijos numeris)

_____
(sudarymo vieta)

Aš, _____,
(vardas ir pavardė)
dirbantis (-ti) _____

_____,
(darbovietės pavadinimas, pareigos)

patvirtinu,
kad esu susipažinęs (-usi) su Valstybinės reikšmės ir pavojingų objektų registro nuostatais, Valstybinės reikšmės ir pavojingų objektų registro duomenų saugos nuostatų ir saugos politiką įgyvendinančių dokumentų reikalavimais.

Pasižadu:
1. Tvarkyti Valstybinės reikšmės ir pavojingų objektų registro (toliau – Registras) duomenis tik tada ir tik tiek, kiek tai būtina nustatytoms funkcijoms atlikti.
2. Vykdyti Valstybinės reikšmės ir pavojingų objektų registro duomenų saugos nuostatų ir kitų saugos politiką įgyvendinančių dokumentų reikalavimus.
3. Neatskleisti ir neperduoti patikėtos ar darbo metu sužinotos Registro informacijos asmenims, kurie nėra įgalioti su ja susipažinti.
4. Nedelsdamas pranešti tiesioginiam vadovui arba tiesiogiai Registro saugos įgaliotiniui apie patikėtos Registro informacijos praradimą ar atskleidimą, taip pat kitus Registro informacijos saugos reikalavimų pažeidimus.
5. Užkirsti kelią neteisėtoms kitų asmenų veikoms, dėl kurių Registro informacija gali būti atskleista, prarasta, sunaikinta, pagrobta ar kitaip neteisėtai įgyta, ir apie šiuos faktus, kitas informacijos atskleidimo ar praradimo aplinkybes nedelsdamas pranešti tiesioginiam vadovui arba tiesiogiai Registro saugos įgaliotiniui.

_____ _____ _____
(pareigos) (parašas) (vardas ir pavardė)

_____

PATVIRTINTA
Priešgaisrinės apsaugos ir gelbėjimo
departamento prie Vidaus reikalų
ministerijos direktoriaus
2016 m. sausio 4 d.
įsakymu Nr. 1/2015-412

VALSTYBINĖS REIKŠMĖS IR PAVOJINGŲ OBJEKTŲ REGISTRO SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės reikšmės ir pavojingų objektų registro saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Tvarkymo taisyklės) nustato tvarką, pagal kurią turi būti saugiai tvarkoma Valstybinės reikšmės ir pavojingų objektų registro (toliau – Registras) elektroninė informacija.

2. Tvarkymo taisyklėse vartojamos sąvokos atitinka Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas), Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. IV-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“ (toliau – Techniniai elektroninės informacijos saugos reikalavimai), Valstybinės reikšmės ir pavojingų objektų registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2000 m. lapkričio 8 d. nutarimu Nr. 1386 „Dėl Pavojingų Lietuvos ūkio objektų registro reorganizavimo į Valstybinės reikšmės ir pavojingų objektų registrą“, Valstybinės reikšmės ir pavojingų objektų registro duomenų saugos nuostatuose, patvirtintuose Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos (toliau – PAGD) direktoriaus 2007 m. birželio 29 d. įsakymu Nr. 1-207 (toliau – Saugos nuostatai) ir kituose saugų elektroninės informacijos bei duomenų tvarkymą reglamentuojančiuose teisės aktuose apibrėžtas sąvokas.

3. Registro elektroninė informacija skirstoma į grupes. Tam tikrai grupei priskirtos Registro elektroninės informacijos sąrašas ir už šios informacijos tvarkymą atsakingi asmenys pateikiami lentelėje:

Eil. Nr.	Registro elektroninės informacijos grupė ir jai priskirta elektroninė informacija	Registro elektroninės informacijos svarbos kategorija	Asmuo, atsakingas už šios informacijos tvarkymą
1.	Registro administravimo (technologiniai) duomenys		
1.1.	Registro duomenys, įvardyti Techninių elektroninės informacijos saugos reikalavimų	Trečia	Administratorius

Eil. Nr.	Registro elektroninės informacijos grupė ir jai priskirta elektroninė informacija	Registro elektroninės informacijos svarbos kategorija	Asmuo, atsakingas už šios informacijos tvarkymą
	5.2, 6.4, 7.6, 7.7 papunkčiuose;		
1.2.	Registro naudotojų duomenys: 1.2.1. Prisijungimo prie Registro identifikatorius 1.2.2. Vardas ir pavardė 1.2.3. Prisijungimo prie Registro pradinis slaptažodis 1.2.4. Darbovietė ir einamosios pareigos 1.2.5. Judriojo ryšio telefonas 1.2.6. Elektroninio pašto adresas 1.2.7. Naudotojui suteiktos prieigos teisės 1.2.8. Prieigos teisių suteikimo, pakeitimo, panaikinimo data	Trečia	Administratorius
2.	Registro bendrieji duomenys, nurodyti Nuostatų 13.1 papunktyje	Antra	Registro naudotojas – tik peržiūra, vidinis Registro naudotojas - tvarkymas
3.	Registro specialieji duomenys, nurodyti Nuostatų 13.2 papunktyje	Antra	Registro naudotojas – tik peržiūra, vidinis Registro naudotojas - tvarkymas
4.	Registre naudojamų klasifikatorių duomenys, nurodyti Nuostatų 14, 15 punktuose	Trečia	Registro naudotojas – tik peržiūra, vidinis Registro naudotojas - tvarkymas

4. Už Tvarkymo taisyklių įgyvendinimo kontrolę atsakingas saugos įgaliotinis.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

5. Siekiant užtikrinti Registro elektroninės informacijos saugą, taikomos šios kompiuterinės įrangos saugos priemonės:

5.1. Registro techninė ir programinė įranga prižiūrima laikantis gamintojo rekomendacijų;

5.2. visa Registro techninė įranga, esanti Registro tarnybinių stočių patalpose ir vidinių Registro naudotojų darbo vietose, įnešama ir išnešama iš jų tik dalyvaujant sisteminiam administratoriui. Jeigu techninė įranga yra perduodama, atiduodama remontuoti arba nurašyti, sisteminis administratorius sunaikina visą techninėje įrangoje esančią elektroninę informaciją, esant būtinumui, daromos techninėje įrangoje esančios elektroninės informacijos kopijos;

5.3. vidinių Registro naudotojų, administratorių kompiuteriai ir kita Registro techninė įranga naudojami tik su tiesioginių pareigų atlikimu susijusiai veiklai vykdyti;

5.4. keičiant kompiuterizuotos darbo vietos paskirtį, visa joje saugoma elektroninė informacija sunaikinama;

5.5. techninės įrangos keitimą, atnaujinimą, priežiūrą ir gedimų šalinimą Registro tarnybinėse stotyse, administratorių ir vidinių Registro naudotojų kompiuterizuotose darbo vietose atlieka sisteminis administratorius arba kvalifikuoti paslaugų teikėjai dalyvaujant administratoriui. Sisteminis administratorius tvarko Registro techninės įrangos keitimų, atnaujinimų, priežiūros ir gedimų šalinimų apskaitos elektroninį žurnalą;

5.6. vidiniams Registro naudotojams draudžiama savavališkai keisti ar kitaip pažeisti esamą techninę įrangą arba jungti asmeninius įrenginius prie Registro vidaus duomenų perdavimo tinklo;

5.7. svarbiausia Registro kompiuterinė įranga ir duomenų perdavimo tinklo mazgai turi įtampos filtrą ir rezervinį maitinimo šaltinį, užtikrinantį šios įrangos veikimą ne mažiau kaip 30 min.;

5.8. vidinių Registro naudotojų darbo vietose naudojamos tik tarnybinėms reikmėms skirtos išorinės duomenų laikmenos (pavyzdžiui, USB, CD/DVD, ir. kt.). Šios laikmenos nenaudojamos veiklai, nesusijusiai su teisėtu Registro tvarkymu.

6. Siekiant užtikrinti Registro elektroninės informacijos saugą, taikomos šios sisteminės ir taikomosios programinės įrangos saugos priemonės:

6.1. visose Registro tarnybinėse stotyse, administratorių ir vidinių Registro naudotojų kompiuterizuotose darbo vietose diegiama saugi programinė įranga, t. y. naudojamos tik gamintojų palaikomos programinės įrangos versijos, kurioms gamintojai reguliariai išleidžia atnaujinimus;

6.2. sisteminis administratorius reguliariai, ne rečiau kaip kartą per savaitę, naudodamas specialią programinę įrangą, įvertina informaciją apie naujus rekomenduojamus gamintojų atnaujinimus, jų reikšmę saugai ir jų įdiegimo būtinumą ir galimybes;

6.3. visose Registro tarnybinėse stotyse, administratorių, Registro naudotojų kompiuterizuotose darbo vietose operacinių sistemų ir taikomųjų programų sąranka parenkama taip, kad būtų užtikrintas didžiausias saugos lygis (išjungiami nereikalingi darbui procesai ir reikmenys (angl. *services*), ribojama arba išjungiama prieiga prie operacinės sistemos prievadų);

6.4. vidinių Registro naudotojų kompiuterių paskyros yra apribotų teisių, kurios neleidžia įdiegti papildomos programinės įrangos. Registro naudotojams negali būti suteikiamos administratoriaus teisės;

6.5. Registro naudotojas unikaliai identifikuojamas (asmens kodas negali būti naudojamas kaip Registro naudotojo identifikatorius) per katalogų valdymo paslaugą (angl. *Active Directory*);

6.6. visose Registro tarnybinėse stotyse, administratorių ir vidinių Registro naudotojų kompiuterizuotose darbo vietose sukuriamos kompiuterių naudotojų paskyros, apsaugotos slaptažodžiais. Slaptažodžių sudarymo, galiojimo trukmės ir jų keitimo reikalavimai aprašomi Valstybinės reikšmės ir pavojingų objektų registro naudotojų administravimo taisyklėse;

6.7. visose Registro tarnybinėse stotyse naudojamos vykdomojo kodo kontrolės priemonės, automatiškai apribojančios ar informuojančios apie neautorizuoto programinio kodo vykdymą;

6.8. naudojama Registro kompiuterinė įranga, kuri automatiškai perspėja sisteminį administratorių apie svarbiausioje Registro kompiuterinėje įrangoje nustatytą laisvos kompiuterio atminties ar vietos standžiajame diske sumažėjimą iki nustatytos pavojingos ribos, apie ilgai neįprastai apkraunamą centrinį procesorių ar kompiuterių tinklo sąsają;

6.9. Registro priežiūros funkcijos atliekamos naudojant atskirą tam skirtą administratoriaus paskyrą, kuria naudojantis negalima atlikti Registro naudotojo funkcijos;

6.10. nuotolinis prisijungimas prie Registro vykdomas protokolu, skirtu duomenims šifruoti.

7. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

7.1. prisijungti prie Registro galima naudojant tik:

7.1.1. HTTPS (angl. *Hypertext Transfer Protocol over Secure Socket Layer*) protokolą – prisijungti Registro naudotojams prie Registro duomenų teikimo puslapio iš viešųjų ryšio tinklų;

7.1.2. HTTPS, FTP (angl. *File Transfer Protocol*) protokolus – prisijungti Registro naudotojams prie Registro iš Vidaus reikalų telekomunikacinio tinklo;

7.1.3. HTTPS, FTP, RDP (angl. *Remote Desktop Protocol*) protokolus – prisijungti prie Registro iš administratorių kompiuterizuotų darbo vietų;

7.1.4. VPN (angl. *virtual private network*) – prisijungti prie Vidaus reikalų telekomunikacinio tinklo naudojant nešiojamuosius administratorių ir Registro naudotojų kompiuterius;

7.2. Registro užkardų (angl. *Firewall*) reikalavimai:

7.2.1. sisteminis administratorius ne rečiau kaip kartą per savaitę analizuoja užkardų įvykių žurnalus (angl. *Logs*) ir kartu su Registro saugos įgaliotiniu reguliariai, tačiau ne rečiau kaip kartą per metus peržiūri ir atnaujina užkardos saugumo taisykles;

7.2.2. pagrindinėse Registro tarnybinėse stotyse, administratorių ir vidinių Registro naudotojų kompiuterizuotose darbo vietose užkardos sukonfigūruotos praleisti tik su Registro funkcionalumu ir administravimu susijusį duomenų srautą. Užkardų konfigūracijų dokumentacija saugoma kartu su informacinės sistemos dokumentacija;

7.2.3. už duomenų perdavimo tinklo užkardų priežiūrą, užkardų valdymo sistemos priežiūrą ir tinkamą užkardų sąranką yra atsakingas sisteminis administratorius;

7.3. Registro duomenų perdavimo tinklo mazgams naudojamas rezervinis maitinimo šaltinis, užtikrinantis šios įrangos veikimą ne mažiau kaip 30 min;

7.4. Registro duomenų perdavimo tinklo perimetro apsaugai naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių vidinių Registro naudotojų kompiuterinę įrangą nuo kenksmingo kodo.

8. Registro saugai užtikrinti yra taikomos šios patalpų ir aplinkos saugumo užtikrinimo priemonės:

8.1. visose Registro patalpose, kur yra vidinių Registro naudotojų, administratorių ir Registro techninė įranga, įrengti gaisro ir įsilaužimo davikliai, kurie prijungti prie pastato signalizacijos ir apsaugos tarnybų;

8.2. patalpos priskiriamos administracinei saugumo zonai. Patekimas prie vidinių Registro naudotojų ir administratorių darbo vietų kontroliuojamas. Nustatyta patalpų raktų saugojimo ir reagavimo į apsauginės ir gaisro aptikimo ir signalizavimo sistemos suveikimą tvarka (numatyti apsaugos darbuotojo (-ų) veiksmai);

8.3. Registro tarnybinių stočių saugai užtikrinti yra taikomos šios patalpų, kuriose yra Registro tarnybinės stotys, ir aplinkos saugumo užtikrinimo priemonės:

8.3.1. į šias patalpas gali patekti tik įgaliotieji asmenys, kitus asmenis lydi įgaliotieji asmenys. Įgaliotųjų asmenų sąrašas tvirtinamas atskiru PAGD direktoriaus įsakymu. Patekimas į tarnybinių stočių patalpas kontroliuojamas ir registruojamas. Kontrolei užtikrinti naudojama įrengta PAGD patalpose įeigos kontrolės sistema. Registracijos duomenys saugomi 14 dienų;

8.3.2. visos išorinės durys ir langai tinkamai apsaugomi nuo neleistinos prieigos (šarvuotos durys be užrašo ant jų, apsaugotos bent dviem skirtingos konstrukcijos spynomis, yra apsauginės žaliuzės;

8.3.3. patalpos atitinka tarnybinių stočių patalpų gaisrinės saugos reikalavimus (įrengta gaisro aptikimo ir signalizavimo sistema ir gaisro gesinimo įranga). Priešgaisrinė signalizacija prijungta prie bendros pastato signalizacijos ir apsaugos tarnybos stebėjimo pulto;

8.3.4. patalpose įrengta apsauga nuo užliejimo iš viršuje esančių patalpų ir vandens aptikimo bei pašalinimo sistema;

8.3.5. patalpose užtikrinamos gamintojo rekomenduojamos techninės įrangos darbo sąlygos (įrengiama oro kondicionavimo ir drėgmės kontrolės įranga);

8.3.6. patalpose įrengiamas elektros maitinimo tinklas, apsaugotas nuo ilgalaikių (daugiau kaip 30 min.) elektros tiekimo iš miesto elektros tinklų sutrikimų (naudojamas autonominis elektros generatorius). Nuo trumpalaikių elektros tiekimo sutrikimų ir įtampos svyravimų tarnybinės stotys ir duomenų perdavimo įranga apsaugomos nenutrūkstamo elektros maitinimo šaltiniais. Maitinimo šaltinis turi perspėjimo apie elektros tiekimo sutrikimus funkciją;

8.3.7. įrengiama stebėsenos sistema, automatiškai informuojanti sisteminį administratorių apie įrangos, aplinkos, duomenų perdavimo tinklo, elektros tinklų ir kitus kritinius pokyčius.

9. Kitos priemonės, naudojamos elektroninės informacijos saugai užtikrinti:

9.1. Registro programinė įranga testuojama naudojant atskirą testavimui skirtą aplinką;

9.2. svarbiausia Registro kompiuterinė įranga, duomenų perdavimo tinklo mazgai ir ryšio linijos yra dubliuoti ir jų techninė būklė nuolat stebima naudojant specializuotą programinę įrangą;

9.3. administratoriai ir Registro naudotojai užtikrina tvarką savo darbo vietoje;

9.4. administratoriai ir Registro naudotojai, baigę darbą ar pasitraukę iš savo darbo vietos, turi užtikrinti, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys ir imasi šių priemonių:

9.4.1. trumpam palikdami savo darbo vietą, atsijungia nuo Registro arba užrakina savo kompiuterį (angl. *lock computer*), arba įjungia ekrano užsklandą (angl. *screen saver*) su slaptažodžiu (režimo aktyvinimo laikas – ne daugiau kaip 15 minučių) ir užrakina kabineto duris (jei išeina iš kabineto);

9.4.2. duomenų laikmenas, dokumentus, jų kopijas, kitas priemones padeda į pašaliniams asmenims neprieinamą vietą;

9.4.3. baigę darbą išjungia kompiuterį;

9.4.4. patikrina, ar patikimai uždaryti langai ir durys, išeidami iš kabineto užrakina duris, pagal Registro tvarkytojo nustatytą tvarką atlieka apsauginės signalizacijos įjungimo veiksmus ir kt.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

10. Elektroninės informacijos peržiūrą, įrašymą, keitimą ir panaikinimą gali atlikti tik atsakingi už šios informacijos tvarkymą asmenys, kaip tai numatyta Tvarkymo taisyklių 3 punkte.

11. Registro naudotojų veiksmų registravimo tvarka:

11.1. Registro naudotojų tapatybė ir veiksmai su Registro duomenimis fiksuojami programinėmis priemonėmis;

11.2. Registre įrašomi ir saugomi duomenys apie Registre įrašomus duomenis, Registro tarnybinių stočių, Registro taikomosios programinės įrangos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis Registro tarnybinėse stotyse, Registro taikomojoje programinėje įrangoje, visus Registro naudotojų vykdomus veiksmus, kitus elektroninės informacijos saugai svarbius įvykius, nurodant Registro naudotojo identifikatorių ir elektroninės informacijos saugai svarbaus įvykio ar vykdyto veiksmo laiką. Šie duomenys saugomi Valstybinės priešgaisrinės gelbėjimo tarnybos informacinėje sistemoje. Šie registracijos duomenys saugomi vienus metus ir paskui sunaikinami. Administratorius vieną kartą per savaitę analizuoja šiuos duomenis;

11.3. Registro posistemiai naudoja įvestos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemones.

12. Atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarka:

12.1. atsarginių kopijų darymo ir atkūrimo reikalavimai aprašyti Saugos nuostatų 28 punkte;

12.2. kopijos saugomos kitose patalpose, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate. Į šias patalpas gali patekti tik įgaliotieji asmenys, kitus asmenis lydi įgaliotieji asmenys. Įgaliotųjų asmenų sąrašas tvirtinamas atskiru PAGD direktoriaus

įsakymu. Patekimas į patalpas kontroliuojamas ir registruojamas. Kontrolei užtikrinti naudojama įrengta PAGD patalpose įeigos kontrolės sistema. Registracijos duomenys saugomi 14 dienų;

12.3. elektroninė informacija kopijose yra užšifruojama (šifravimo raktai saugomi atskirai nuo kopijų) arba imamasi kitų priemonių, neleidžiančių panaudoti kopijų neteisėtai elektroninei informacijai atkurti;

12.4. Registro programinė įranga registruoja kopijų darymo istoriją;

12.5. atsarginės laikmenos su Registro programinės įrangos kopijomis laikomos nedegioje spintoje kitose patalpose arba kitame pastate, nei yra Registro tarnybinės stotys. Patekimas į patalpas, kuriose laikomos programinės įrangos kopijos, kontroliuojamas.

12.6. už Registro duomenų kopijavimą, saugojimą ir atkūrimą atsako sisteminis administratorius;

12.7. už atsarginių duomenų saugojimo kontrolę atsakingas saugos įgaliotinis;

12.8. už savo kompiuterizuotose darbo vietose esančių duomenų išsaugojimą atsakingi Registro naudotojai.

13. Registro duomenys teikiami kitiems registrams, kadastrams bei informacinėms sistemoms ir iš jų gaunami pagal duomenų teikimo sutartis, kuriose įskaitant, bet neapsiribojant, nurodoma informacijos saugumo ir slaptumo sąlygos, teikiamų arba iš jų gaunamų duomenų sąrašai, duomenų teikimo arba gavimo juridinis pagrindas, duomenų teikimo arba gavimo ir naudojimo tikslas, duomenų teikimo arba gavimo ir naudojimo tvarka ir sąlygos, prieigos prie Registro arba kitų registrų, kadastrų ir informacinių sistemų leistinas būdas ir laikas, atsakomybės ir ginčų sprendimo tvarka, duomenų teikimo sutarties galiojimo terminas ir sąlygos. Registro duomenų teikimo ir gavimo sutartys derinamos su saugos įgaliotiniu.

14. Elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo nustatymo tvarka:

14.1. sisteminis administratorius naudoja visas įmanomas aparatines, programines ir administracines priemones, skirtas Registro duomenims nuo neleidžiamos veiklos apsaugoti;

14.2. kilus įtarimui, kad su Registru arba jame saugomais ir apdorojamais duomenimis yra vykdoma neleidžiama veikla, sisteminis administratorius nedelsdamas privalo apie tai informuoti saugos įgaliotinį;

14.3. saugos įgaliotinis, gavęs pranešimą apie neleidžiamą veiklą ir įvertinęs neleidžiamos veiklos galimus padarinius Registro veiklai, gali paskelbti elektroninės informacijos saugos incidentą ir imtis jo šalinimo veiksmų nustatytų Registro veiklos tęstinumo valdymo plane.

15. Programinės ir techninės įrangos keitimo ir atnaujinimo tvarka:

15.1. prieš atlikdamas Registro programinės ir techninės įrangos keitimą, kurio metu gali iškilti grėsmė Registro elektroninės informacijos konfidencialumui, vientisumui ar pasiekiamumui, sisteminis administratorius išbando planuojamus Registro pakeitimus atskiroje testavimo aplinkoje, kurioje esantys asmens duomenys naudojami, vadovaudamasis Valstybės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymo Nr. 1T-71(1.12) „Dėl bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms patvirtinimo“ 10.10 papunkčio reikalavimu;

15.2. sėkmingai atlikęs Registro programinės ir techninės įrangos pakeitimų bandymus, sisteminis administratorius gali pradėti keisti Registro programinę ir techninę įrangą;

15.3. planuodamas Registro programinės arba techninės įrangos keitimą, kurio metu galimi Registro veikimo sutrikimai, sisteminis administratorius iš anksto elektroniniu paštu informuoja Registro naudotojus apie tokių darbų pradžią ir galimus Registro veikimo sutrikimus;

15.4. sisteminis administratorius Registro naudotojams iš anksto pateikia visą reikalingą informaciją apie naudojimosi Registru pokyčius, kurių atsiradimas susijęs su įvykdytais arba vykdomais Registro pakeitimais.

16. Registro pokyčių valdymo tvarka nurodyta Registro valdytojo patvirtintame Registro pokyčių valdymo tvarkos apraše.

17. Nešiojamuosius kompiuterius ir kitus mobiliuosius įrenginius galima naudoti tik su einamosiomis pareigomis susijusiai veiklai. Nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių, skirtų Registro elektroninei informacijai tvarkyti, naudojimo ne Registro tvarkytojo patalpose tvarka pateikta Saugos nuostatų 26 punkte.

IV SKYRIUS
REIKALAVIMAI, KELIAMI REGISTRUI FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

18. Paslaugų teikėjų prieigos prie Registro lygiai ir sąlygos:

18.1. paslaugų teikėjui suteikiama tik tokia prieiga prie Registro techninės ir programinės įrangos, kuri paslaugų teikėjo įgaliotam atsakingam asmeniui būtina sutartyse numatytiems įsipareigojimams vykdyti;

18.2. paslaugų teikėjo įgalioti atsakingi asmenys supažindinami su prieigos prie Registro sąlygomis, elektroninės informacijos saugos reikalavimais ir atsakomybe, numatomas reikalavimas pasirašyti konfidencialumo susitarimą arba pasižadėjimą;

18.3. pasibaigus sutartyje nurodytam įsipareigojimų vykdymo laikotarpiui, duomenų tvarkymo administratorius panaikina paslaugų teikėjo įgaliotų atsakingų asmenų prieigas prie Registro.

19. Patalpų, įrangos, informacinių sistemų, duomenų perdavimo tinklų projektavimo, diegimo ir priežiūros paslaugų reikalavimai nustatomi šių paslaugų teikimo sutartyse, atsižvelgiant į:

19.1. atitiktį Registro keliamiems saugos reikalavimams;

19.2. Registro turimos ir planuojamos įdiegti įrangos suderinamumą;

19.3. suderinamumą su kitomis Registro valdytojo valdomomis informacinėmis sistemomis ir registrais, naudojama technine ir programine įranga.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

20. Tvarkymo taisyklės yra privalomos Registro naudotojams, saugos įgaliotiniui ir administratoriams.

21. Registro naudotojai privalo kuo greičiau informuoti administratorių arba saugos įgaliotinį apie pastebėtus šių Tvarkymo taisyklių reikalavimų pažeidimus, Registro veiklos sutrikimus arba neįprastą Registro veikimą.

22. Registro naudotojai, saugos įgaliotinis ar administratoriai, pažeidę šių Tvarkymo taisyklių ar kitų saugos politiką įgyvendinančių dokumentų reikalavimus, atsako teisės aktų nustatyta tvarka.

_____

PATVIRTINTA
Priešgaisrinės apsaugos ir gelbėjimo
departamento prie Vidaus reikalų
ministerijos direktoriaus
2016 m. sausio 4 d.
įsakymu Nr. 1/2015-412

VALSTYBINĖS REIKŠMĖS IR PAVOJINGŲ OBJEKTŲ REGISTRO VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės reikšmės ir pavojingų objektų registro veiklos tęstinumo valdymo plano (toliau – Valdymo planas) tikslas – nustatyti Valstybinės reikšmės ir pavojingų objektų registro (toliau – Registras) sisteminių administratorių, duomenų tvarkymo administratorių (toliau – administratoriai), saugos įgaliotinio, Registro naudotojų ir kitų asmenų veiksmus, įvykus elektroninės informacijos saugos incidentui, kurio metu iškyla pavojus Registro duomenims, Registro techninės, programinės įrangos funkcionavimui.

2. Valdymo plane vartojamos sąvokos atitinka 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“, Valstybinės reikšmės ir pavojingų objektų registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2000 m. lapkričio 8 d. nutarimu Nr. 1386 „Dėl Valstybinės reikšmės ir pavojingų objektų registro nuostatų patvirtinimo“, Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos valdomų valstybės informacinių sistemų ir Valstybinės reikšmės ir pavojingų objektų registro duomenų saugos nuostatuose, patvirtintuose Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus 2019 m. spalio 4 d. įsakymu Nr. 1-414, ir kituose saugų elektroninės informacijos ir duomenų tvarkymą reglamentuojančiuose teisės aktuose apibrėžtas sąvokas.

Punkto pakeitimai:
Nr. 1-472, 2019-11-15, paskelbta TAR 2019-11-15, i. k. 2019-18335

3. Registro naudotojai, pastebėję saugos dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai sisteminiam administratoriui ir saugos įgaliotiniui.

4. Saugos įgaliotinis, įtaręs neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeisiančią Registro saugą, skelbia elektroninės informacijos saugos incidentą ir apie tai praneša Veiklos tęstinumo valdymo grupei.

5. Valdymo planas įsigalioja įvykus elektroninės informacijos saugos incidentui.

6. Registro elektroninės informacijos saugos incidento tyrimas atliekamas pagal Registro elektroninės informacijos saugos incidentų tyrimų tvarkos aprašą (1 priedas).

7. Administratoriai, saugos įgaliotinis, Registro naudotojai ir kiti asmenys elektroninės informacijos saugos incidento metu turi visus įgaliojimus atlikti veiksmus, nurodytus Registro veiklos atkūrimo detaliajame plane (Valdymo plano 2 priedas). Administratoriai, saugos įgaliotinis, prireikus – Registro naudotojai nedelsdami šalina elektroninės informacijos saugos incidento padarinius ir įgyvendina kitas detaliajame plane numatytus veiksmus.

8. Šis Valdymo planas privalomas Registro tvarkytojui, valdytojui, saugos įgaliotiniui, administratoriams, Registro naudotojams.

9. Registro veiklos atkūrimas, įvykus elektroninės informacijos saugos incidentui, finansuojamas iš Lietuvos Respublikos valstybės biudžeto ir kitų finansavimo šaltinių. Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos (toliau – PAGD) finansavimo plane numatomi finansiniai ištekliai, kurių pakaktų elektroninės informacijos saugos incidentui pašalinti ne ilgiau nei per 12 valandų ir Valdymo plano 10 punkte nurodytiems kriterijams užtikrinti.

Punkto pakeitimai:

Nr. 1-472, 2019-11-15, paskelbta TAR 2019-11-15, i. k. 2019-18335

10. Registro veiklos kriterijai, pagal kuriuos galima nustatyti, ar Registro veikla atkurta, yra šie:

10.1. Registro naudotojai gali atlikti savo darbines funkcijas įprastiniu būdu;

10.2. užtikrintas duomenų tvarkomų Registre prieinamumas, konfidencialumas ir vientisumas;

10.3. Registras vykdo Registro nuostatuose ir kituose teisės aktuose nurodytus uždavinius ir funkcijas;

10.4. per metus užtikrintas Registro prieinamumas ne mažiau kaip 96 proc. laiko visą parą.

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

11. Elektroninės informacijos saugos incidentams valdyti ir veiklai atkurti sudaromos dvi grupės: Veiklos tęstinumo valdymo grupė (toliau – Valdymo grupė) ir Veiklos atkūrimo grupė.

12. Valdymo grupė – užtikrina veiklos tęstinumui kylančių grėsmių valdymą ir Registro atkūrimo koordinavimą įvykus elektroninės informacijos saugos incidentui.

13. Registro Valdymo grupės sudėtis:

13.1. PAGD Civilinės saugos valdybos viršininkas – Valdymo grupės vadovas;

13.2. PAGD Materialinių išteklių ir logistikos grupės patarėjas – Valdymo grupės vadovo pavaduotojas;

13.3. PAGD Pajėgų valdymo valdybos Veiklos organizavimo skyriaus viršininkas;

13.4. PAGD Planavimo ir projektų valdymo skyriaus vedėjas;

13.5. PAGD Finansų skyriaus vedėjas;

13.6. PAGD Teisės ir personalo skyriaus vedėjas;

13.7. PAGD Viešųjų pirkimų skyriaus vedėjas;

13.8. saugos įgaliotinis.

Punkto pakeitimai:

Nr. 1-472, 2019-11-15, paskelbta TAR 2019-11-15, i. k. 2019-18335

14. Pagrindinė Registro Valdymo grupės pasitarimų vieta – PAGD posėdžių salė (401 kabinetas, 1 korpusas, Švitrigailos g. 18, Vilnius). Alternatyvi Registro Valdymo grupės pasitarimų vieta – Valstybės ekstremaliųjų situacijų operacijų centro slėptuvė (2 korpusas, Švitrigailos g. 18, Vilnius).

Punkto pakeitimai:

Nr. 1-472, 2019-11-15, paskelbta TAR 2019-11-15, i. k. 2019-18335

15. Valdymo grupės nariai, gavę informaciją iš saugos įgaliotinio apie įvykusį elektroninės informacijos saugos incidentą, susisiekia su Valdymo grupės vadovu ir kuo skubiau susirenka į Valdymo grupės pasitarimų vietą, jei Valdymo grupės vadovas nenurodė kitos susirinkimo vietos.

16. Valdymo grupė atlieka šias funkcijas:

16.1. analizuoja elektroninės informacijos saugos incidentus ir priima sprendimus Registro veiklos tęstinumo valdymo klausimais;

16.2. bendrauja su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;

16.3. bendrauja su kitų informacinių sistemų veiklos tęstinumo valdymo grupėmis;

16.4. bendrauja su teisėsaugos ir kitomis institucijomis, šių institucijų darbuotojais ir kitais suinteresuotais asmenimis;

16.5. atlieka finansinių ir kitų išteklių, reikalingų Registro veiklai atkurti įvykus elektroninės informacijos saugos incidentui, naudojimo kontrolę;

16.6. organizuoja Registro duomenų fizinę saugą, įvykus elektroninės informacijos saugos incidentui;

16.7. organizuoja logistiką (žmonių, daiktų, įrangos vežimo organizavimas ir jų vežimas);

16.8. vykdo Registro veiklos atkūrimo priežiūrą ir koordinavimą;

16.9. duoda žodinius ir rašytinius nurodymus, kurie yra privalomi visiems PAGD darbuotojams.

17. Veiklos atkūrimo grupė vykdo Registro atkūrimo darbus ir Valdymo grupės nurodymus susijusius su Registro funkcionalumo atkūrimu.

18. Veiklos atkūrimo grupės sudėtis:

18.1. PAGD Civilinės saugos valdybos Civilinės saugos planavimo ir koordinavimo skyriaus viršininkas – Veiklos atkūrimo grupės vadovas;

18.2. PAGD Informacinių technologijų ir ryšių skyriaus vedėjas – Veiklos atkūrimo grupės vadovo pavaduotojas;

18.3. PAGD Pajėgų valdymo valdybos Veiklos organizavimo skyriaus, PAGD Civilinės saugos valdybos Gyventojų apsaugos organizavimo skyriaus ir PAGD Informacinių technologijų ir ryšių skyriaus darbuotojai (Registro administratoriai).

Punkto pakeitimai:

Nr. 1-472, 2019-11-15, paskelbta TAR 2019-11-15, i. k. 2019-18335

19. Esant poreikiui ir suderinus su Registro Valdymo grupe, Veiklos atkūrimo grupės funkcijoms vykdyti galima pasitelkti papildomus Registro valdytojo, tvarkytojo ar kitų subjektų žmogiškuosius išteklius.

20. Registro Veiklos atkūrimo grupės funkcijos ir asmenys, atsakingi už šių funkcijų vykdymą:

20.1. tarnybinių stočių veikimo atkūrimo organizavimas (atsakingi Veiklos atkūrimo grupės vadovas ir sisteminiai administratoriai);

20.2. kompiuterių tinklo veikimo atkūrimo organizavimas (atsakingi Veiklos atkūrimo grupės vadovo pavaduotojas ir sisteminiai administratoriai);

20.3. Registro ir jo posistemių elektroninės informacijos atkūrimo organizavimas (atsakingi Veiklos atkūrimo grupės vadovas ir sisteminiai administratoriai);

20.4. taikomųjų programų tinkamo veikimo atkūrimo organizavimas (atsakingi Veiklos atkūrimo grupės vadovas, sisteminiai ir duomenų tvarkymo administratoriai);

20.5. kompiuterių ir kitos techninės įrangos veikimo atkūrimo ir prisijungimo prie kompiuterių tinklo organizavimas (atsakingi Veiklos atkūrimo grupės vadovo pavaduotojas ir sisteminiai administratoriai).

21. Įvykus elektroninės informacijos saugos incidentui Valdymo grupė ir Veiklos atkūrimo grupė vadovaujasi Registro veiklos tęstinumo detaliuoju planu, kuris pateikiamas šio Valdymo plano 2 priede.

22. Valdymo grupė ir Veiklos atkūrimo grupė tarpusavyje ir su kitomis grupėmis bendrauja naudodamosi elektroninių ryšių priemonėmis: elektroniniu paštu, mobiliuoju ryšiu ir kitomis įmanomomis ryšio priemonėmis. Bendravimo dažnumas priklauso nuo Registro elektroninės informacijos saugos incidento masto, pobūdžio ir veiklos atkūrimo eigos, tačiau grupės privalo

komunikuoti ne rečiau kaip vieną kartą per 6 val., kol bus pašalinti elektroninės informacijos saugos incidento padariniai.

23. Įvykus elektroninės informacijos saugos incidentui, visi Valdymo grupės ir Veiklos atkūrimo grupės nariai visą parą pasiekiami mobiliuoju telefonu.

24. Jeigu pagrindinės Registro patalpos, kuriose yra Registro tarnybinės stotys ir kita telekomunikacinė įranga, yra netinkamos, siekiant užtikrinti Registro veiklą įvykus elektroninės informacijos saugos incidentui, naudojamos atsarginės Registro atkūrimo patalpos. Numatoma vieta – Informatikos ir ryšio departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos (Šventaragio g. 2, Vilnius).

25. Atsarginės patalpos atitinka pagrindinėms patalpoms keliamus reikalavimus, kurie nurodyti Valstybinės reikšmės ir pavojingų objektų registro saugaus elektroninės informacijos tvarkymo taisyklėse.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

26. Parengti ir saugomi dokumentai:

26.1. Registro techninės ir programinės įrangos specifikacija;

26.2. Registro minimalaus funkcionalumo techninės ir programinės įrangos specifikacija;

26.3. Registro techninės įrangos išdėstymo brėžiniai;

26.4. Registro kompiuterių tinklo fizinio ir loginio sujungimo schemų rinkinys;

26.5. Registro duomenų teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąrašas;

26.6. Registro programinės įrangos laikmenų ir laikmenų su atsarginėmis programinės įrangos kopijomis saugojimo žurnalas;

26.7. Registro Veiklos tęstinumo valdymo grupės ir Registro Veiklos atkūrimo grupės narių sąrašas.

Punkto pakeitimai:
Nr. 1-472, 2019-11-15, paskelbta TAR 2019-11-15, i. k. 2019-18335

27. Registro techninės ir programinės įrangos specifikacijoje pateikta informacija apie Registro techninę ir programinę įrangą ir jos parametrus. Už Registro techninės ir programinės įrangos priežiūrą yra atsakingas sisteminis administratorius. Elektroninės informacijos incidento metu nesant sisteminio administratoriaus (dėl komandiruotės, ligos ar kitų priežasčių), jį pavaduojančio asmens minimalus kompetencijos ar žinių lygis negali būti žemesnis už sisteminiam administratoriui keliamų reikalavimų lygį. Minimalūs reikalavimai sisteminiam administratoriui yra nurodyti Registro saugos nuostatuose.

28. Registro minimalaus funkcionalumo techninės ir programinės įrangos specifikacijoje pateikta informacija apie minimalaus funkcionalumo techninės ir programinės įrangos, tinkamos Registro tvarkymo įstaigos poreikius atitinkančiai veiklai užtikrinti elektroninės informacijos saugos incidento metu, specifikaciją.

29. Registro techninės įrangos išdėstymo brėžiniuose pateikti kiekvieno pastato, kuriame yra Registro įranga, aukšto patalpų brėžiniai su juose pažymėtais tarnybinėmis stotimis, kompiuterių tinklo ir telefonų tinklo mazgais, kompiuterių tinklo ir telefonų tinklo laidų vedimo tarp pastato aukštų vietomis ir elektros įvedimo pastate vietomis.

30. Registro kompiuterių tinklo fizinio ir loginio sujungimo schemų rinkinyje pateiktos Registro kompiuterių tinklo fizinio ar loginio sujungimo schemos.

31. Registro duomenų teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąraše pateiktos duomenų teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutartys ir atsakingų už šių sutarčių įgyvendinimo priežiūrą asmenų pareigos.

32. Registro programinės įrangos laikmenų ir laikmenų su atsarginėmis programinės įrangos kopijomis saugojimo žurnale nurodyta programinės įrangos laikmenų ir laikmenų su atsarginėmis programinės įrangos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos.

33. Veiklos tęstinumo valdymo grupės ir Veiklos atkūrimo grupės narių sąraše nurodytas Veiklos tęstinumo valdymo grupės ir Veiklos atkūrimo grupės narių sąrašas, kuriame pateikti mobiliojo, darbo ir namų telefono numeriai ir gyvenamosios vietos adresai.

IV SKYRIUS
PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

34. Veiklos tęstinumo valdymo plano veiksmingumas išbandomas ne rečiau kaip kartą per metus, data numatoma atliekant Registro saugos atitikties vertinimą. Numatytu laiku imituojamas elektroninės informacijos saugos incidentas, kurio metu už elektroninės informacijos saugos incidento padarinių likvidavimą atsakingi asmenys atlieka minėtų padarinių likvidavimo veiksmus. Saugos įgaliotinis turi teisę inicijuoti neplaninį Valdymo plano veiksmingumo išbandymą.

35. Plano veiksmingumo išbandymo rezultatus saugos įgaliotinis išdėsto ataskaitoje (Valdymo plano 3 priedas), kurioje aprašomi pastebėti trūkumai ir pateikiami pasiūlymai dėl pastebėtų trūkumų šalinimo. Parengtą ataskaitą saugos įgaliotinis pateikia Registro valdytojo vadovui.

36. Plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami laikantis operatyvumo, veiksmingumo ir ekonomiškumo principų.

_____

Valstybinės reikšmės ir pavojingų objektų
registro veiklos tęstinumo valdymo plano
1 priedas

VALSTYBINĖS REIKŠMĖS IR PAVOJINGŲ OBJEKTŲ REGISTRO ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTŲ TYRIMO TVARKOS APRAŠAS

1. Įvykus elektroninės informacijos saugos incidentui, saugos įgaliotinis surenka informaciją apie incidento vietą, požymius, laiką, padarinius ir kitus su incidentu susijusius duomenis, pateikia visa turimą informaciją Veiklos tęstinumo valdymo grupei.

2. Likvidavus elektroninės saugos incidento sukeltus padarinius, saugos įgaliotinis dokumentuoja visą surinktą informaciją. Elektroninės informacijos saugos incidentas, Registro atkuriamieji darbai ir juose dalyvavę, sutrikimus pašalinę darbuotojai registruojami elektroninės informacijos saugos incidentų žurnale (Valdymo plano 4 priedas).

3. Užpildytą elektroninės informacijos saugos incidentų registravimo žurnalą ir kitą su incidentu susijusią informaciją saugos įgaliotinis pateikia Registro veiklos tęstinumo valdymo grupei.

4. Registro veiklos tęstinumo valdymo grupė apsvarsčiusi turimą informaciją apie incidentą, jo padarinius, atliktus atkuriamuosius darbus ir Registro patirtą žalą, priima sprendimus dėl priemonių įgyvendinimo, kurios ateityje leistų išvengti panašaus pobūdžio elektroninės informacijos saugos incidentų pasikartojimo arba sumažintų galimą jų padarytą žalą.

5. Registro veiklos tęstinumo valdymo grupės priimtus sprendimus saugos įgaliotinis pateikia Registro valdytojo vadovui.

_____

Valstybinės reikšmės ir pavojingų objektų
registro veiklos tęstinumo valdymo plano
2 priedas

VALSTYBINĖS REIKŠMĖS IR PAVOJINGŲ OBJEKTŲ REGISTRO VEIKLOS ATKŪRIMO DETALUSIS PLANAS

Pavojaus rūšys, sukeliančios incidentą	Veiklos atkūrimo veiksmai	Įgaliotieji vykdytojai
1. Gamtos veiksniai ir jų padariniai (smarkus lietus, labai smarki audra, škvalas, kruša, smarkus speigas)	1.1. specialiųjų tarnybų informavimas, jeigu būtina;	pavojų pastebėjęs Registro darbuotojas
	1.2. saugos įgaliotinio ir Veiklos tęstinumo valdymo grupės nario informavimas;	pavojų pastebėjęs Registro darbuotojas
	1.3. Veiklos tęstinumo valdymo grupės vadovo ir narių informavimas ir susitikimo pasitarimų vietoje organizavimas;	saugos įgaliotinis
	1.4. darbuotojų evakavimo organizavimas, jeigu būtina;	Veiklos tęstinumo valdymo grupės vadovas
	1.5. nurodymų ir rekomendacijų iš specialiųjų tarnybų gavimas;	Veiklos tęstinumo valdymo grupės vadovas
	1.6. galimybės dirbti pavojaus vietoje svarstymas;	Veiklos tęstinumo valdymo grupės vadovas
	1.7. darbuotojų informavimas apie nurodymus ir rekomendacijas, galimybes dirbti pavojaus vietoje;	Veiklos tęstinumo valdymo grupės vadovo pavaduotojas
	1.8. nuostolių, padarytų patalpoms, jų įtakos Registro veiklai ir iš to išplaukiančių padarinių įvertinimas;	Veiklos tęstinumo valdymo grupės vadovas
	1.8. visų įmanomų priemonių, siekiant apsaugoti svarbiausią Registro įrangą ir duomenis, įgyvendinimas;	Veiklos atkūrimo grupės vadovas
	1.9. nuostolių, padarytų Registro įrangai ir duomenims, įvertinimas;	Veiklos tęstinumo valdymo grupės vadovas
	1.10. Registro nuostolių likvidavimo priemonių plano sudarymas ir paskelbimas;	Veiklos tęstinumo valdymo grupės vadovas
	1.11. Registro nuostolius likviduojančių darbuotojų paskyrimas ir jų veiksmų koordinavimas;	Veiklos atkūrimo grupės vadovas
	1.12. Registro veiklos perkėlimas į atsargines Registro atkūrimo patalpas, jeigu būtina;	Veiklos atkūrimo grupės vadovas
	1.13. sugadintos ar prarastos įrangos atkūrimas, remontuojant ar įsigyjant naują;	Veiklos atkūrimo grupės vadovas, sisteminis administratorius
	1.14. Registro duomenų atkūrimas iš atsarginių kopijų ir veiklos atkūrimas duomenų praradimo ar sugadinimo atveju;	sisteminis administratorius
	1.15. įvykusio incidento analizė ir Veiklos tęstinumo valdymo plano pakeitimai, siekiant išvengti panašių situacijų arba jų padarinių ateityje.	saugos įgaliotinis, Veiklos tęstinumo valdymo grupės vadovas
2. Gaisras	2.1. gaisro gesinimas ankstyvojoje stadijoje, jeigu yra galimybė;	pavojų pastebėjęs Registro darbuotojas

Pavojaus rūšys, sukeliančios incidentą	Veiklos atkūrimo veiksmai	Įgaliotieji vykdytojai
	2.2. priešgaisrinės gelbėjimo tarnybos informavimas;	pavojų pastebėjęs Registro darbuotojas
	2.3. Registro saugos įgaliotinio ir Veiklos tęstinumo valdymo grupės nario informavimas;	pavojų pastebėjęs Registro darbuotojas
	2.4. Veiklos tęstinumo valdymo grupės vadovo ir narių informavimas ir susitikimo pasitarimų vietoje organizavimas;	saugos įgaliotinis
	2.5. darbuotojų evakavimo organizavimas;	Veiklos tęstinumo valdymo grupės vadovas
	2.6. nurodymų ir rekomendacijų iš priešgaisrinės gelbėjimo tarnybos gavimas;	Veiklos tęstinumo valdymo grupės vadovas
	2.7. galimybės dirbti pavojaus vietoje svarstymas;	Veiklos tęstinumo valdymo grupės vadovas
	2.8. darbuotojų informavimas apie nurodymus ir rekomendacijas, galimybes dirbti pavojaus vietoje;	Veiklos tęstinumo valdymo grupės vadovo pavaduotojas
	2.9. komunikacijų ir įrangos, galinčių sukelti pavojų, išjungimas;	Veiklos atkūrimo grupės vadovas
	2.10. nuostolių, padarytų patalpoms, jų įtakos Registro veiklai ir iš to išplaukiančių padarinių įvertinimas;	Veiklos tęstinumo valdymo grupės vadovas
	2.11. visų įmanomų priemonių, siekiant apsaugoti svarbiausią Registro įrangą ir duomenis, įgyvendinimas;	Veiklos atkūrimo grupės vadovas
	2.12. nuostolių, padarytų Registro įrangai ir duomenims, įvertinimas;	Veiklos atkūrimo grupės vadovas
	2.13. Registro nuostolių likvidavimo priemonių plano sudarymas ir paskelbimas;	Veiklos tęstinumo valdymo grupės vadovas
	2.14. Registro nuostolius likviduojančių darbuotojų paskyrimas ir jų veiksmų koordinavimas;	Veiklos atkūrimo grupės vadovas
	2.15. Registro veiklos perkėlimas į atsargines Registro atkūrimo patalpas, jeigu būtina;	Veiklos atkūrimo grupės vadovas
	2.16. sugadintos ar prarastos įrangos atkūrimas, remontuojant ar įsigyjant naują;	Veiklos atkūrimo grupės vadovas, sisteminis administratorius
	2.17. Registro duomenų atkūrimas iš atsarginių kopijų ir veiklos atkūrimas duomenų praradimo ar sugadinimo atveju;	sisteminis administratorius
	2.18. įvykusio incidento analizė ir Veiklos tęstinumo valdymo plano pakeitimai, siekiant išvengti panašių situacijų arba jų padarinių ateityje.	saugos įgaliotinis, Veiklos tęstinumo valdymo grupės vadovas
3. Patalpų pažeidimas arba praradimas	3.1. specialiųjų tarnybų informavimas;	pavojų pastebėjęs Registro darbuotojas
	3.2. saugos įgaliotinio ir Veiklos tęstinumo valdymo grupės nario informavimas;	pavojų pastebėjęs Registro darbuotojas
	3.3. Veiklos tęstinumo valdymo grupės vadovo ir	saugos įgaliotinis

Pavojaus rūšys, sukeliančios incidentą	Veiklos atkūrimo veiksmai	Įgaliotieji vykdytojai
	narių informavimas, susitikimo pasitarimų vietoje organizavimas;	
	3.4. darbuotojų evakavimo organizavimas;	Veiklos tęstinumo valdymo grupės vadovas
	3.5. nurodymų ir rekomendacijų iš specialiųjų tarnybų gavimas;	Veiklos tęstinumo valdymo grupės vadovas
	3.6. galimybės dirbti pavojaus vietoje svarstymas;	Veiklos tęstinumo valdymo grupės vadovas
	3.7. darbuotojų informavimas apie nurodymus ir rekomendacijas, galimybes dirbti pavojaus vietoje;	Veiklos tęstinumo valdymo grupės vadovo pavaduotojas
	3.8. patalpose esančios įrangos išjungimas ir užrakinimas, jeigu yra galimybė;	Veiklos atkūrimo grupės vadovas
	3.9. patalpų apsaugos organizavimas;	Veiklos tęstinumo valdymo grupės vadovas
	3.10. nuostolių, padarytų patalpoms, jų įtakos Registro veiklai ir iš to išplaukiančių padarinių įvertinimas;	Veiklos tęstinumo valdymo grupės vadovas
	3.11. nuostolių, padarytų Registro įrangai ir duomenims, įvertinimas;	Veiklos atkūrimo grupės vadovas
	3.12. Registro nuostolių likvidavimo priemonių plano sudarymas ir paskelbimas;	Veiklos tęstinumo valdymo grupės vadovas
	3.13. Registro nuostolius likviduojančių darbuotojų paskyrimas ir jų veiksmų koordinavimas;	Veiklos atkūrimo grupės vadovas
	3.14. Registro veiklos perkėlimas į atsargines Registro atkūrimo patalpas;	Veiklos atkūrimo grupės vadovas
	3.15. pažeistų patalpų remonto, renovacijos arba atkūrimo organizavimas;	Veiklos tęstinumo valdymo grupės vadovas
	3.16. sugadintos ar prarastos įrangos atkūrimas remontuojant ar įsigyjant naują;	Veiklos atkūrimo grupės vadovas, sisteminis administratorius
	3.17. Registro duomenų atkūrimas iš atsarginių kopijų ir veiklos atkūrimas duomenų praradimo ar sugadinimo atveju;	sisteminis administratorius
	3.18. įvykusio incidento analizė ir Veiklos tęstinumo valdymo plano pakeitimai, siekiant išvengti panašių situacijų arba jų padarinių ateityje.	saugos įgaliotinis, Veiklos tęstinumo valdymo grupės vadovas
4. Elektros energijos tiekimo sutrikimai	4.1. saugos įgaliotinio ir Veiklos tęstinumo valdymo grupės nario informavimas;	pavojų pastebėjęs Registro darbuotojas
	4.2. Veiklos tęstinumo valdymo grupės vadovo ir narių informavimas, susitikimo pasitarimų vietoje organizavimas;	saugos įgaliotinis
	4.3. elektros energijos tiekimo sutrikimo priežasčių nustatymas;	Veiklos tęstinumo valdymo grupės vadovas
	4.4. kreipimasis į elektros energijos tiekėją dėl sutrikimo pašalinimo trukmės ir galimybių;	Veiklos tęstinumo valdymo grupės vadovas

Pavojaus rūšys, sukeliančios incidentą	Veiklos atkūrimo veiksmai	Įgaliotieji vykdytojai
	4.5. informacijos ir rekomendacijų iš elektros energijos tiekėjo gavimas;	Veiklos tęstinumo valdymo grupės vadovas
	4.6. tarnybinių stočių ir kitos techninės įrangos alternatyvaus elektros energijos tiekimo užtikrinimas;	Veiklos atkūrimo grupės vadovas
	4.7. alternatyvaus elektros energijos tiekimo įrenginio (generatoriaus) ir nepertraukiamo maitinimo šaltinių priežiūra;	Veiklos atkūrimo grupės vadovas
	4.8. elektros energijos tiekimo sutrikimo poveikio svarbiausiai Registro įrangai ir duomenims įvertinimas;	Veiklos atkūrimo grupės vadovas
	4.9. Registro nuostolių likvidavimo priemonių plano sudarymas ir paskelbimas, jeigu būtina;	Veiklos tęstinumo valdymo grupės vadovas
	4.10. Registro nuostolius likviduojančių darbuotojų paskyrimas ir jų veiksmų koordinavimas, jeigu būtina;	Veiklos atkūrimo grupės vadovas
	4.11. Registro duomenų atkūrimas iš atsarginių kopijų ir veiklos atkūrimas duomenų praradimo ar sugadinimo atveju;	sisteminis administratorius
	4.12. įvykusio incidento analizė ir Veiklos tęstinumo valdymo plano pakeitimai, siekiant išvengti panašių situacijų arba jų padarinių ateityje.	saugos įgaliotinis, Veiklos tęstinumo valdymo grupės vadovas
5. Vandentiekio arba šildymo sistemos sutrikimai	5.1. saugos įgaliotinio ir Veiklos tęstinumo valdymo grupės nario informavimas;	pavojų pastebėjęs Registro darbuotojas
	5.2. Veiklos tęstinumo valdymo grupės vadovo ir narių informavimas, susitikimo pasitarimų vietoje organizavimas;	saugos įgaliotinis
	5.3. vandentiekio arba šildymo komunikacijų atjungimo svarstymas ir iniciavimas;	Veiklos tęstinumo valdymo grupės vadovas
	5.4. kreipimasis į vandentiekio arba šildymo paslaugų tiekėją dėl sutrikimo pašalinimo trukmės ir galimybių;	Veiklos tęstinumo valdymo grupės vadovas
	5.5. darbuotojų informavimas apie sutrikimą ir elgesio patalpose rekomendacijas;	Veiklos tęstinumo valdymo grupės vadovo pavaduotojas
	5.6. sutrikimo priežasčių nustatymas;	Veiklos tęstinumo valdymo grupės vadovas
	5.7. sutrikimo poveikio svarbiausiai Registro įrangai ir duomenims įvertinimas;	Veiklos atkūrimo grupės vadovas
	5.8. Registro nuostolių likvidavimo priemonių plano sudarymas ir paskelbimas, jeigu būtina;	Veiklos tęstinumo valdymo grupės vadovas
	5.9. Registro nuostolius likviduojančių darbuotojų paskyrimas ir jų veiksmų koordinavimas, jeigu būtina;	Veiklos atkūrimo grupės vadovas
	5.10. Registro veiklos perkėlimas į atsargines Registro atkūrimo patalpas, jeigu būtina;	Veiklos atkūrimo grupės vadovas
	5.11. vandentiekio arba šildymo tiekimo paslaugų	Veiklos tęstinumo

Pavojaus rūšys, sukeliančios incidentą	Veiklos atkūrimo veiksmai	Įgaliotieji vykdytojai
	atnaujinimo organizavimas;	valdymo grupės vadovas
	5.12. Registro veiklos atkūrimas, atnaujinus vandentiekio ir šildymo paslaugų tiekimą, jeigu būtina;	Veiklos atkūrimo grupės vadovas
	5.13. įvykusio incidento analizė ir Veiklos tęstinumo valdymo plano pakeitimai, siekiant išvengti panašių situacijų arba jų padarinių ateityje.	saugos įgaliotinis, Veiklos tęstinumo valdymo grupės vadovas
6. Ryšio sutrikimai	6.1. saugos įgaliotinio ir Veiklos tęstinumo valdymo grupės nario informavimas;	pavojų pastebėjęs Registro darbuotojas
	6.2. Veiklos tęstinumo valdymo grupės vadovo ir narių informavimas, susitikimo pasitarimų vietoje organizavimas;	saugos įgaliotinis
	6.3. ryšio sutrikimo priežasčių nustatymas;	Veiklos tęstinumo valdymo grupės vadovas
	6.4. kreipimasis į ryšio paslaugų teikėją dėl sutrikimo pašalinimo trukmės;	Veiklos tęstinumo valdymo grupės vadovas
	6.5. darbuotojų informavimas dėl ryšio sutrikimo;	Veiklos tęstinumo valdymo grupės vadovo pavaduotojas
	6.6. kreipimasis į alternatyvų ryšio paslaugų teikėją, jeigu sutrikimas nepašalintas;	Veiklos tęstinumo valdymo grupės vadovas
	6.7. įvykusio incidento analizė ir Veiklos tęstinumo valdymo plano pakeitimai, siekiant išvengti panašių situacijų arba jų padarinių ateityje.	saugos įgaliotinis, Veiklos tęstinumo valdymo grupės vadovas
7. Techninės įrangos sugadinimas, netekimas arba funkcionavimo sutrikimai	7.1. saugos įgaliotinio ir Veiklos tęstinumo valdymo grupės nario informavimas;	pavojų pastebėjęs Registro darbuotojas
	7.2. Veiklos tęstinumo valdymo grupės vadovo ir narių informavimas, susitikimo pasitarimų vietoje organizavimas;	saugos įgaliotinis
	7.3. pranešimas teisėsaugos tarnybai apie įvykį vagystės arba vandalizmo atveju;	Veiklos tęstinumo valdymo grupės vadovas
	7.4. bendravimas su teisėsaugos tarnyba vykstant įvykio tyrimui;	Veiklos tęstinumo valdymo grupės vadovas
	7.5. darbuotojų informavimas apie techninės įrangos sutrikimus;	Veiklos tęstinumo valdymo grupės vadovo pavaduotojas
	7.6. techninės įrangos gedimų nustatymas;	Veiklos atkūrimo grupės vadovas, sisteminis administratorius
	7.7.sugadintos techninės įrangos atkūrimo galimybių įvertinimas;	Veiklos atkūrimo grupės vadovas
	7.8. netektos techninės įrangos pakeitimo galimybių naujas įvertinimas;	Veiklos atkūrimo grupės vadovas
	7.9. nuostolių, padarytų Registro įrangai ir duomenims, įvertinimas;	Veiklos atkūrimo grupės vadovas
	7.10. Registro nuostolių likvidavimo priemonių plano	Veiklos tęstinumo

Pavojaus rūšys, sukeliančios incidentą	Veiklos atkūrimo veiksmai	Įgaliotieji vykdytojai
	sudarymas ir paskelbimas;	valdymo grupės vadovas
	7.11. Registro nuostolius likviduojančių darbuotojų paskyrimas ir jų veiksmų koordinavimas;	Veiklos atkūrimo grupės vadovas
	7.12. esamų techninės įrangos išteklių perskirstymas, siekiant kompensuoti praradimą;	Veiklos atkūrimo grupės vadovas
	7.13. sugadintos ar prarastos techninės įrangos atkūrimas, remontuojant ar įsigyjant naują;	Veiklos atkūrimo grupės vadovas, sisteminis administratorius
	7.14. Registro duomenų atkūrimas iš atsarginių kopijų ir veiklos atkūrimas duomenų praradimo ar sugadinimo atveju;	sisteminis administratorius
	7.15. įvykusio incidento analizė ir Veiklos tęstinumo valdymo plano pakeitimai, siekiant išvengti panašių situacijų arba jų padarinių ateityje.	saugos įgaliotinis, Veiklos tęstinumo valdymo grupės vadovas
8. Programinės įrangos sugadinimas, duomenų praradimas	8.1. saugos įgaliotinio ir Veiklos tęstinumo valdymo grupės nario informavimas;	pavojų pastebėjęs Registro darbuotojas, Registro naudotojas
	8.2. Veiklos tęstinumo valdymo grupės vadovo ir narių informavimas, susitikimo pasitarimų vietoje organizavimas;	saugos įgaliotinis
	8.3. darbuotojų informavimas apie veiklos sutrikimus arba prarastus duomenis;	Veiklos tęstinumo valdymo grupės vadovo pavaduotojas
	8.4. prarastų duomenų apimties ir praradimo priežasčių nustatymas;	Veiklos tęstinumo valdymo grupės vadovas, sisteminis administratorius
	8.5. pranešimas teisėsaugos tarnybai, jeigu su Registro duomenimis buvo atliktos neteisėtos veikos;	Veiklos tęstinumo valdymo grupės vadovas
	8.6. bendravimas su teisėsaugos tarnyba vykstant įvykio tyrimui;	Veiklos tęstinumo valdymo grupės vadovas
	8.7. nuostolių, padarytų Registrui, ir iš to išplaukiančių padarinių įvertinimas;	Veiklos tęstinumo valdymo grupės vadovas
	8.8. Registro nuostolių likvidavimo priemonių plano sudarymas ir paskelbimas;	Veiklos tęstinumo valdymo grupės vadovas
	8.9. Registro nuostolius likviduojančių darbuotojų paskyrimas ir jų veiksmų koordinavimas;	Veiklos atkūrimo grupės vadovas
	8.10. Registro duomenų atkūrimas iš atsarginių kopijų ir veiklos atkūrimas;	sisteminis administratorius
	8.11. Registro saugumo spragų pašalinimas, jeigu dėl jų kaltės duomenys buvo prarasti;	Veiklos atkūrimo grupės vadovas
	8.12. įvykusio incidento analizė ir Veiklos tęstinumo valdymo plano pakeitimai, siekiant išvengti panašių situacijų arba jų padarinių ateityje.	saugos įgaliotinis, Veiklos tęstinumo valdymo grupės vadovas
9. Įsilaužimas į vidinį tinklą	9.1. saugos įgaliotinio ir Veiklos tęstinumo valdymo grupės nario informavimas;	pavojų pastebėjęs Registro darbuotojas,

Pavojaus rūšys, sukeliančios incidentą	Veiklos atkūrimo veiksmai	Įgaliotieji vykdytojai
(kibernetinė ataka)		Registro naudotojas
	9.2. Veiklos tęstinumo valdymo grupės vadovo ir narių informavimas, susitikimo pasitarimų vietoje organizavimas;	saugos įgaliotinis
	9.3. Registro veiklos sutrikimo dėl įsilaužimo į vidinį kompiuterių tinklą priežasčių ir trikdžių šaltinio identifikavimas;	Veiklos tęstinumo valdymo grupės vadovas
	9.4. pranešimas apie įvykį elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo tarnybai, nustačius įsilaužimą į Vidaus reikalų ministerijos telekomunikacinį tinklą iš išorės;	Veiklos tęstinumo valdymo grupės vadovas
	9.5. darbuotojų informavimas apie Registro veiklos sutrikimus;	Veiklos tęstinumo valdymo grupės vadovo pavaduotojas
	9.6. nuostolių, padarytų Registro duomenims, ir iš to išplaukiančių padarinių įvertinimas;	Veiklos tęstinumo valdymo grupės vadovas
	9.7. Registro nuostolių likvidavimo priemonių plano sudarymas ir paskelbimas;	Veiklos tęstinumo valdymo grupės vadovas
	9.8. Registro nuostolius likviduojančių darbuotojų paskyrimas ir jų veiksmų koordinavimas;	Veiklos atkūrimo grupės vadovas
	9.9. Registro duomenų atkūrimas iš atsarginių kopijų ir veiklos atkūrimas duomenų praradimo ar sugadinimo atveju;	sisteminis administratorius
	9.10. alternatyvaus svarbių duomenų perdavimo būdo kompiuteriniais tinklais organizavimas ir duomenų perdavimo saugumo užtikrinimas.	Veiklos atkūrimo grupės vadovas
	9.11. Registro saugumo spragų pašalinimas, jeigu dėl jų kaltės buvo įsilaužta į vidinį kompiuterių tinklą;	Veiklos atkūrimo grupės vadovas
	9.12. įvykusio incidento analizė ir Veiklos tęstinumo valdymo plano pakeitimai, siekiant išvengti panašių situacijų arba jų padarinių ateityje.	saugos įgaliotinis, Veiklos tęstinumo valdymo grupės vadovas

_____

Valstybinės reikšmės ir pavojingų objektų registro veiklos tęstinumo valdymo plano 3 priedas

VALSTYBINĖS REIKŠMĖS IR PAVOJINGŲ OBJEKTŲ REGISTRO VEIKLOS TĘSTINUMO VALDYMO PLANO BANDYMO ATASKAITA

_____
(data)

Elektroninės informacijos saugos incidento scenarijus:	
Funkcijos ir posistemiai, kuriuos paveikė elektroninės informacijos saugos incidentas:	
Elektroninės informacijos saugos incidento šalinimo eiga:	
Rasti Registro veiklos tęstinumo valdymo plano trūkumai:	
Pasiūlymai keisti arba papildyti Registro veiklos tęstinumo valdymo planą:	

Bandant Valstybinės reikšmės ir pavojingų objektų registro veiklos tęstinumo valdymo planą dalyvavo:

Vardas, pavardė	Parašas
1.	
2.	
3.	
4.	
5.	

Valstybinės reikšmės ir pavojingų objektų registro
veiklos tęstinumo valdymo plano
4 priedas

(Valstybinės reikšmės ir pavojingų objektų registro elektroninės informacijos saugos incidentų registravimo žurnalo formos pavyzdys)

VALSTYBINĖS REIKŠMĖS IR PAVOJINGŲ OBJEKTŲ REGISTRO ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTŲ REGISTRAVIMO ŽURNALAS

Eil. Nr.	Elektroninės informacijos saugos incidentas						
	požymio kodas	pradžia (metai, mėnuo, diena, valanda)	pabaiga (metai, mėnuo, diena, valanda)	įvykio aprašymas	atkuriamieji darbai	pašalino (vardas ir pavardė)	saugos įgaliotinis (vardas ir pavardė, parašas)

Elektroninės informacijos saugos incidento situacijos požymiai:
1. gamtos veiksniai ir jų padariniai; 2. gaisras; 3. patalpų pažeidimas arba praradimas; 4. elektros energijos tiekimo sutrikimai; 5. vandentiekio arba šildymo sistemos sutrikimai; 6. ryšio sutrikimai; 7. techninės įrangos sugadinimas, netekimas arba funkcionavimo sutrikimai; 8. programinės įrangos sugadinimas, duomenų praradimas; 9. įsilaužimas į vidinį kompiuterių tinklą arba kibernetinė ataka.

Pakeitimai:

1.
Priešgaisrinės apsaugos ir gelbėjimo departamentas prie Vidaus reikalų ministerijos, Įsakymas
Nr. 1-414, 2019-10-04, paskelbta TAR 2019-10-04, i. k. 2019-15863
Dėl Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos valdomų valstybės informacinių sistemų ir valstybinės reikšmės ir pavojingų objektų registro duomenų saugos nuostatų patvirtinimo

2.
Priešgaisrinės apsaugos ir gelbėjimo departamentas prie Vidaus reikalų ministerijos, Įsakymas
Nr. 1-472, 2019-11-15, paskelbta TAR 2019-11-15, i. k. 2019-18335
Dėl Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus 2016 m. sausio 4 d. įsakymo Nr. 1/2015-412 „Dėl Valstybinės reikšmės ir pavojingų objektų registro duomenų saugos nuostatų, Valstybinės

reikšmės ir pavojingų objektų registro saugaus elektroninės informacijos tvarkymo taisyklių, Valstybinės reikšmės ir pavojingų objektų registro naudotojų administravimo taisyklių ir Valstybinės reikšmės ir pavojingų objektų registro veiklos tęstinumo valdymo plano patvirtinimo“ pakeitimo