

Suvestinė redakcija nuo 2018-11-01

Įsakymas paskelbtas: Žin. 2012, Nr. [107-5440](#), i. k. 112301MISAK00D1-730

**LIETUVOS RESPUBLIKOS APLINKOS MINISTRO
Į S A K Y M A S****DĖL LIETUVOS RESPUBLIKOS UPIŲ, EŽERŲ IR TVENKINIŲ VALSTYBĖS
KADASTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO**

2012 m. rugsėjo 11 d. Nr. D1-730
Vilnius

Vadovaudamasis 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, 11, 19 punktais:

Preambulės pakeitimai:

Nr. [D1-681](#), 2014-08-21, paskelbta TAR 2014-08-25, i. k. 2014-11189

Nr. [D1-877](#), 2018-10-10, paskelbta TAR 2018-10-31, i. k. 2018-17536

1. T v i r t i n u Lietuvos Respublikos upių, ežerų ir tvenkinių valstybės kadastro duomenų saugos nuostatus (pridedama).

2. P a v e d u:

2.1. Aplinkos apsaugos agentūrai paskirti Lietuvos Respublikos upių, ežerų ir tvenkinių valstybės kadastro saugos įgaliotiniai;

2.2. Aplinkos ministerijos Informacinių technologijų skyriui ne vėliau kaip per 1 mėnesį nuo šio įsakymo įsigaliojimo dienos pateikti aplinkos ministru tvirtinti Lietuvos Respublikos upių, ežerų ir tvenkinių valstybės kadastro saugaus elektroninės informacijos tvarkymo taisyklės, Lietuvos Respublikos upių, ežerų ir tvenkinių valstybės kadastro veiklos tęstinumo valdymo planą ir Lietuvos Respublikos upių, ežerų ir tvenkinių valstybės kadastro naudotojų administravimo taisyklės.

APLINKOS MINISTRAS

GEDIMINAS KAZLAUSKAS

SUDERINTA

Lietuvos Respublikos vidaus reikalų ministerijos
2011-10-20 raštu Nr. 1D-7248(3)

PATVIRTINTA

Lietuvos Respublikos aplinkos ministro
2012 m. rugsėjo 11 d. įsakymu Nr. D1-730
(Lietuvos Respublikos aplinkos ministro
2014 m. rugpjūčio 21 d. įsakymo Nr. D1-681
redakcija)

**LIETUVOS RESPUBLIKOS
UPIŲ, EŽERŲ IR TVENKINIŲ KADASTRO DUOMENŲ SAUGOS
NUOSTATAI**

I. BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos upių, ežerų ir tvenkinių kadastro (toliau – kadastras) duomenų saugos nuostatų (toliau – Saugos nuostatai) tikslas – sudaryti sąlygas saugiai automatizuotu būdu rinkti, apdoroti, kaupti, tvarkyti kadastro elektroninę informaciją, užtikrinant elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą bei tinkamą registro veikimą.

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

3. Kadastro saugos politiką nustato Saugos nuostatai, kurių įgyvendinamieji dokumentai yra kadastro saugaus elektroninės informacijos tvarkymo taisyklės, kadastro veiklos tęstinumo valdymo planas ir kadastro naudotojų administravimo taisyklės (toliau – Saugos politiką įgyvendinantys dokumentai).

4. Informacijos saugumo užtikrinimo prioritetinės kryptys:

4.1. fizinė informacijos apdorojimo priemonių (elektroninės informacijos perdavimo įrangos, programinės įrangos) apsauga;

4.2. teisėtas, saugus, kokybiškas elektroninės informacijos tvarkymas ir naudojimas;

4.3. kadastro saugos priemonių įgyvendinimas ir kontrolė;

4.4. kadastro veiklos tęstinumas esant elektroninės informacijos saugos incidentams.

5. Kadastro valdytojo ir tvarkytojo pavadinimai ir adresai:

5.1. kadastro valdytojas – Aplinkos ministerija, A. Jakšto g. 4, LT-01105 Vilnius;

5.2. kadastro tvarkytojas – Aplinkos apsaugos agentūra, A. Juozapavičiaus g. 9, LT-09311 Vilnius.

6. Kadastro valdytojo funkcijos, susijusios su kadastro sauga:

6.1. koordinuoja kadastro tvarkytojo darbą, metodiškai jam vadovauja ir įstatymų nustatyta tvarka atlieka šio darbo priežiūrą;

6.2. rengia ir tvirtina teisės aktus, susijusius su kadastro tvarkymu ir duomenų sauga;

6.3. vykdo kadastro duomenų saugos reikalavimų laikymosi priežiūrą;

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

6.5. atsako už kadastro saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą.

6.6. Atsako už serverių tinklų veikimą ir apsaugą.

7. Kadastro tvarkytojo funkcijos, susijusios su kadastro sauga:

7.1. užtikrina kadastro elektroninės informacijos saugą;

7.2. teikia pasiūlymus kadastro valdytojui, kaip tobulinti kadastro saugą;

7.3. užtikrina tinkamą kadastro valdytojo priimtų teisės aktų ir rekomendacijų įgyvendinimą;

7.4. skiria kadastro saugos įgaliotinį;

7.5. skiria kadastro administratorių;

- 7.6. užtikrina registro sąveiką su kitomis informacinėmis sistemomis ir registrais;
- 7.7. kadastro tvarkytojo vadovas yra atsakingas už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka.
8. Saugos įgaliotinio funkcijos, susijusios su kadastro sauga:
- 8.1. teikia kadastro tvarkytojo įstaigos vadovui pasiūlymus dėl administratorių skyrimo;
- 8.2. teikia kadastro valdytojo vadovui siūlymus dėl saugos dokumentų priėmimo, keitimo ar pripažinimo netekusiais galios, atlieka kadastro saugos reikalavimų atitikties vertinimą;
- 8.3. koordinuoja elektroninės informacijos saugos incidentų kadastre tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklą, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais, išskyrus atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės;
- 8.4. teikia administratoriui privalomus vykdyti nurodymus ir pavedimus;
- 8.5. periodiškai inicijuoja kadastro naudotojų mokymą informacijos saugos klausimais, informuoja juos apie informacijos saugos problematiką;
- 8.6. atlieka kitas kadastro valdytojo ir tvarkytojo vadovų pavestas ir kituose teisės aktuose jam priskirtas funkcijas;
- 8.7. įgyvendindamas elektroninės informacijos saugą, kadastro saugos įgaliotinis negali atlikti administratoriaus funkcijų ir yra atsakingas už tinkamą Saugos nuostatuose nustatytų funkcijų vykdymą.
9. Administratorius atlieka šias funkcijas, susijusias su kadastro sauga:
- 9.1. įvertina kadastro naudotojų pasirengimą dirbti su informacine sistema ir suteikia kadastro naudotojams teisę naudotis informacinės sistemos galimybėmis paskirtoms funkcijoms atlikti;
- 9.2. rengia pasiūlymus kadastro palaikymo, priežiūros ir duomenų saugos klausimais;
- 9.3. administruoja kadastro komponentus (kompiuterius, operacines sistemas), nustato pažeidžiamų vietų ir saugos reikalavimų atitiktį;
- 9.4. atlieka kadastro naudotojų kompiuterinių darbo vietų programinės įrangos priežiūrą, kontrolę ir užtikrina tinkamą veikimą;
- 9.5. atlieka funkcijas, susijusias su saugumo reikalavimų atitikties nustatymu ir stebėseną, reagavimu į elektroninės informacijos saugos incidentus, vykdo saugos įgaliotinio nurodymus ir pavedimus, susijusius su kadastro saugos užtikrinimu ir nuolat teikti informaciją saugos įgaliotiniui apie saugą užtikrinančių pagrindinių komponentų būklę.
10. Saugų kadastro duomenų tvarkymą reglamentuoja:
- 10.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;
- 10.2. 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, kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL 2016 L 119, p. 1);
- 10.3. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Bendrieji reikalavimai);
- 10.4. Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų

turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo aprašo patvirtinimo“;

10.5. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“ (toliau – Techniniai saugos reikalavimai);

10.6. Saugos dokumentų turinio gairių aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo—gairių aprašo patvirtinimo“ (toliau – Turinio gairės);

10.7. Lietuvos standartai LST ISO/IEC 27002:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ ir LST ISO/IEC 27001: 2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, kiti Lietuvos ir tarptautiniai grupės „Informacijos technologija. Saugumo metodai“ standartai;

10.8. Lietuvos Respublikos upių, ežerų ir tvenkinių kadastro nuostatai, patvirtinti Lietuvos Respublikos Vyriausybės 2000 m. rugsėjo 19 d. nutarimu Nr. 1114 „Dėl Lietuvos Respublikos upių, ežerų ir tvenkinių kadastro steigimo ir jo nuostatų patvirtinimo“ (toliau – kadastro nuostatai);

10.9. kiti teisės aktai, reglamentuojantys elektroninės informacijos saugumo politiką (toliau – saugos politika) ir duomenų tvarkymo teisėtumą, valstybės informacinių sistemų tvarkytojų veiklą ir duomenų saugos valdymą.

Punkto pakeitimai:

Nr. [D1-877](#), 2018-10-10, paskelbta TAR 2018-10-31, i. k. 2018-17536

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

11. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 4.2.3 ir 4.2.4 papunkčių nuostatomis, kadastrė tvarkoma informacija priskirtina svarbios elektroninės informacijos kategorijai.

12. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 5.2 papunkčio nuostatomis, kadastras priskiriamas antrai informacinių sistemų kategorijai.

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

14. Kadastro rizikos vertinimas išdėstomas rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos kadastro duomenų saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtumo kriterijus.

Pagrindiniai rizikos veiksniai yra:

14.1. subjektyvūs netyčiniai – veiksniai, atsirandantys dėl darbo organizavimo nesklaidumų, vidaus tvarkos taisyklių pažeidimų, kadastro administravimo, kontrolės ir priežiūros trūkumų, kadastro naudotojų, kadastro duomenų gavėjų ir teikėjų kontrolės trūkumo, kadastro programinės įrangos klaidų, klaidingų kadastro duomenų įvedimo, darbuotojų praradimo ir kaitos;

14.2. subjektyvūs tyčiniai – nesankcionuotas prisijungimas prie kadastro, klaidingų duomenų įvedimas, operacinės sistemos, operacinės sistemos naudotojo teisių ir taikomosios programinės įrangos pakeitimas, kadastro naudotojų, kadastro duomenų gavėjų ir teikėjų teisių viršijimas, bandymas atspėti slaptažodžius ar kitaip pažeisti taikomas saugos priemonės, piktnaudžiavimas siekiant patogumo (slaptažodžių išsaugojimas kompiuterių atmintyje ir pan.), vidaus tvarkos taisyklių pažeidimas, nesankcionuotas prisijungimas prie vietinio kompiuterių tinklo, kadastro duomenų atskleidimas nesilaikant kadastro nuostatų, kenksmingo kodo ir kitos programinės įrangos, galinčios pakenkti kadastro saugai, naudojimas ar platinimas;

14.3. nenugalima jėga (*force majeure*).

15. Kadastro rizikos veiksniai vertinami nustatant jų įtakos kadastro saugai laipsnius:

15.1. žemas. Duomenų pažeidimo poveikio laipsnis nedidelis, padariniai nebus pavojingi – įvesti netikslūs duomenys, dingę dalis informacijos, kurią galima greitai atstatyti iš atsarginių kopijų, prarasta informacija po paskutinio kopijavimo. Neveikia kompiuterinė programinė įranga ir (ar) operacinė sistema kompiuterizuotose darbo vietose;

15.2. vidutinis. Duomenų pažeidimo poveikio laipsnis gali būti didelis, padariniai rimti – duomenys netikslūs ar sugadinti, bet juos įmanoma atstatyti iš atsarginių kopijų. Duomenų bazių įrašai pakeisti, sunku rasti klaidas ir suklastotą informaciją, neveikia kompiuterinė programinė įranga ir (ar) operacinė sistema tarnybinėse stotyse;

15.3. aukštas. Duomenų pažeidimo poveikio laipsnis labai didelis, padariniai rimti – duomenys visiškai sugadinti, dėl vagystės, gaisro ar užliejimo prarasti ne tik duomenų bazių duomenys, bet ir atsarginės kopijos, neveikia visa Licencijų informacinė sistema.

16. kadastro rizikos vertinimo metu atliekami darbai:

16.1. kadastrą sudarančių informacinių išteklių inventorizacija;

16.2. įtakos kadastro veiklai vertinimas;

16.3. grėsmės ir pažeidimų analizė;

16.4. liekamosios rizikos vertinimas.

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

18. Pagrindiniai elektroninės informacijos saugos priemonių parinkimo principai:

18.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

18.2. informacijos saugos priemonės diegimo kaina turi būti adekvati saugomos informacijos vertei.

18.3. kur galima, turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

19. Programinės įrangos, skirtos informacinei sistemai apsaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir panašiai), naudojimo nuostatos ir jos atnaujinimo reikalavimai:

19.1. tarnybinėse stotyse ir kompiuterizuotose darbo vietose su „Microsoft Windows“ operacine sistema privalo būti įdiegta centralizuotai valdoma apsauga nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos ir kt.);

19.2. antivirusinės programinės įrangos kenksmingo kodo aprašai turi būti atnaujinami ne rečiau kaip kartą per 24 valandas;

19.3. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

20. Programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos:

20.1. kadastro naudotojų kompiuterizuotose darbo vietose įdiegiama legali ir saugi operacinė sistema (su naujausiais pataisymais) bei programinė įranga;

20.2. Apsaugai nuo kenksmingo kodo užtikrinti turi būti nuolat vykdomas kadastro naudotojų kompiuterių ir serverių operacinių sistemų ir taikomųjų programų atnaujinimas.

Operacinės sistemos ir taikomosios programos atnaujinamos vadovaujantis gamintojo rekomendacijomis;

20.3. kadastro naudotojų kompiuterizuotose darbo vietose turi būti naudojama tik su tarnybine veikla susijusi programinė įranga;

20.4. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka administratoriai.

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

21.1. Kompiuterių tinklas, prie kurio prijungti kadastro naudotojų kompiuteriai, nuo viešojo interneto turi būti atskirtas ugniasienėmis;

21.2. visas kadastro duomenų srautas į ir iš interneto yra filtruojamas naudojant apsaugą nuo virusų ir kitos kenkėjiškos programinės įrangos;

21.3. naudojamos aplikacijų kontrolės sistemos.

22. Metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą:

22.1. kadastro duomenų perdavimo duomenų gavėjams būdai, sąlygos ir tvarka nurodyti kadastro nuostatų VI ir VII skyriuose;

22.2. kadastro duomenys perduodami vadovaujantis TCP/IP protokolu, prieiga prie kadastro yra ribojama ugniasienėmis pagal sutartyse numatytus kriterijus (IP adresus).

23. Kadastro naudotojams draudžiama naudoti nešiojamuosius kompiuterius duomenims perduoti kompiuterių tinklais ne savo darbo vietoje. Nešiojamuosiuose kompiuteriuose esanti informacija turi būti apsaugota operacinės sistemos ir naudotojo vardu bei slaptažodžiu.

24. Kadastro naudotojams tiesioginė prieiga prie kadastro duomenų suteikiama nustatant kadastro naudotojų registracijos vardus ir slaptažodžius.

25. Pasibaigus valstybės tarnybos (darbo) santykiams, kadastro naudotojo teisė naudotis kadastro duomenimis turi būti panaikinta.

26. Pagrindiniai atsarginių elektroninės informacijos kopijavimo ir atkūrimo reikalavimai:

26.1. daromos atsarginės elektroninės informacijos kopijos, kurios turi būti laikomos atskiroje patalpoje ir saugomos užrakintoje nedegioje spintoje. Atsarginės duomenų kopijos turi būti daromos ne rečiau kaip kartą per savaitę;

26.2. atkūrimas iš atsarginių kopijų privalo būti išbandomas ne rečiau kaip kartą per metus. Duomenų atkūrimo išbandymą organizuoja administratorius. Reikalavimai kadastro funkcionalumo atstatymui ir prieinamumui:

26.2.1. turi būti užtikrintas pagrindinių informacinės sistemos funkcijų atkūrimas per 8 valandas nuo veiklos sutrikimo;

26.2.2. turi būti užtikrintas informacinės sistemos prieinamumas ne mažiau kaip 90 procentų laiko darbo metu.

IV. REIKALAVIMAI PERSONALUI

27. Visi kadastro naudotojai privalo turėti darbo kompiuteriu įgūdžių, mokėti tvarkyti kadastro duomenis, būti susipažinę su Saugos nuostatais ir saugos politikos įgyvendinimą reglamentuojančiais teisės aktais.

28. Kadastro naudotojai, pažeidę Saugos nuostatų ar kitų saugos politiką įgyvendinančių teisės aktų reikalavimus, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

29. Kadastro saugos įgaliotinis privalo turėti universitetinį informacinių technologijų ar teisės srities išsilavinimą, išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, kitais

Lietuvos Respublikos ir Europos Sąjungos teisės aktais. kadastro saugos įgaliotinis privalo sugebėti prižiūrėti kaip įgyvendinama saugos politika.

30. Kadastro administratorius privalo turėti informacinių technologijų srities išsilavinimą, išmanyti darbą su kompiuterių tinklais, duomenų bazėmis ir mokėti užtikrinti jų saugumą. Kadastro administratorius privalo mokėti administruoti ir prižiūrėti duomenų bazines, būti susipažinęs su Saugos nuostatais ir saugos politiką įgyvendinančiais teisės aktais. Administratorius privalo tobulinti kvalifikaciją elektroninės informacijos saugos srityje, jam turi būti rengiami duomenų saugos mokymai.

31. Kadastro saugos įgaliotinis ne rečiau kaip kartą per dvejus metus inicijuoja kadastro naudotojų mokymą informacijos saugos klausimais.

V. KADASTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

32. Saugos nuostatai ir saugos politiką įgyvendinantys dokumentai skelbiami Aplinkos ministerijos intraneto svetainėje.

33. Saugos įgaliotinis supažindina kadastro naudotojus su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ir atsakomybe už reikalavimų nesilaikymą, informuoja apie minėtų teisės aktų pakeitimus.

34. Pakartotinai su saugos politiką reglamentuojančiais teisės aktais kadastro naudotojai supažindinami tik iš esmės pasikeitus informacijos saugą reglamentuojantiems teisės aktams. Informacija apie pasikeitimus saugos politiką įgyvendinančiuose teisės aktuose siunčiama elektroniniu būdu.

Priedo pakeitimai:

Nr. [D1-681](#), 2014-08-21, paskelbta TAR 2014-08-25, i. k. 2014-11189

Pakeitimai:

1.

Lietuvos Respublikos aplinkos ministerija, Įsakymas

Nr. [D1-681](#), 2014-08-21, paskelbta TAR 2014-08-25, i. k. 2014-11189

Dėl Lietuvos Respublikos aplinkos ministro 2012 m. rugsėjo 11 d. įsakymo Nr. D1-730 „Dėl Lietuvos Respublikos upių, ežerų ir tvenkinių valstybės kadastro duomenų saugos nuostatų patvirtinimo“ pakeitimo

2.

Lietuvos Respublikos aplinkos ministerija, Įsakymas

Nr. [D1-877](#), 2018-10-10, paskelbta TAR 2018-10-31, i. k. 2018-17536

Dėl Lietuvos Respublikos aplinkos ministro 2012 m. rugsėjo 11 d. įsakymo Nr. D1-730 „Dėl Lietuvos Respublikos upių, ežerų ir tvenkinių valstybės kadastro duomenų saugos nuostatų patvirtinimo“ pakeitimo