Elektroninio dokumento nuorašas

NACIONALINĖS ŽEMĖS TARNYBOS PRIE ŽEMĖS ŪKIO MINISTERIJOS DIREKTORIUS

ĮSAKYMAS DĖL NACIONALINĖS ŽEMĖS TARNYBOS PRIE ŽEMĖS ŪKIO MINISTERIJOS DIREKTORIAUS 2011 M. LAPKRIČIO 22 D. ĮSAKYMO NR. 1P-(1.3.)-267 „DĖL ŽEMĖS INFORMACINĖS SISTEMOS NUOSTATŲ IR ŽEMĖS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO

2014 m. spalio 8 d. Nr. 1P-(1.3.)-390

Vilnius

P a k e i č i u Nacionalinės žemės tarnybos prie Žemės ūkio ministerijos direktoriaus 2011 m. lapkričio 22 d. įsakymą Nr. 1P-(1.3.)-267 „Dėl Žemės informacinės sistemos nuostatų ir Žemės informacinės sistemos duomenų saugos nuostatų patvirtinimo“:

1. Pakeičiu preambulę ir ją išdėstau taip:

„Vadovaudamasis Lietuvos Respublikos žemės įstatymo 34 straipsnio 3 dalimi, Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“, 11 punktu ir Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimo aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 7.1 papunkčiu:“

2. Pakeičiu nurodytuoju įsakymu patvirtintus Žemės informacinės sistemos duomenų saugos nuostatus ir išdėstau juos nauja redakcija (pridedama).

Direktoriaus pavaduotojas,
atliekantis direktoriaus funkcijas Vaidas Pakalka

PATVIRTINTA
Nacionalinės žemės tarnybos prie
Žemės ūkio ministerijos direktoriaus
2011 m. lapkričio 22 d. įsakymu
Nr. 1P-(1.3.)-267
(Nacionalinės žemės tarnybos prie
Žemės ūkio ministerijos direktoriaus
2014 m. spalio 8 d. Nr. 1P-(1.3.)-390
redakcija)

ŽEMĖS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Žemės informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Žemės informacinės sistemos (toliau – ŽIS) duomenų saugos politiką, nustato administracines, technines ir kitas priemones, užtikrinančias saugų ŽIS duomenų tvarkymą.

2. Saugos nuostatai parengti vadovaujantis 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“, Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų saugos reikalavimais, patvirtintais 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 valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų saugos reikalavimai).

3. Saugos nuostatuose vartojamos sąvokos:

3.1. **Administratorius** – ŽIS valdytojo valstybės tarnautojas arba ŽIS tvarkytojo darbuotojas, dirbantis pagal darbo sutartį, atliekantis ŽIS priežiūrą;

3.2. **Saugos įgaliotinis** – ŽIS valdytojo paskirtas valstybės tarnautojas, įgyvendinantis ŽIS duomenų saugą;

3.3. **ŽIS naudotojas** – ŽIS valdytojo valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, arba ŽIS tvarkytojo darbuotojas, dirbantis pagal darbo sutartį, kuriems administratorius suteikė teisę naudotis ŽIS ištekliais numatytoms funkcijoms vykdyti.

Kitos šiuose Saugos nuostatuose vartojamos sąvokos atitinka sąvokas, apibrėžtas šių Saugos nuostatų 2 punkte išvardytuose teisės aktuose bei Lietuvos standartuose LST ISO/IEC 27001:2013 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos.

Reikalavimai“ ir LST ISO/IEC 27002:2014 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“.

4. ŽIS duomenų saugos tikslas – užtikrinti ŽIS duomenų vientisumą, prieinamumą ir konfidencialumą bei tinkamą ŽIS infrastruktūros (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, įsilaužimų aptikimo sistemų, duomenų perdavimo tinklų) veikimą.

5. ŽIS duomenų saugumo užtikrinimo prioritetinės kryptys:

5.1. administracinių, techninių ir kitų priemonių, skirtų ŽIS duomenų saugai užtikrinti, įgyvendinimas ir kontrolė;

5.2. veiklos tęstinumo užtikrinimas;

5.3. ŽIS naudotojų mokymas;

5.4. elektroninės informacijos konfidencialumo, prieinamumo ir vientisumo užtikrinimas.

6. ŽIS valdytojo ir tvarkytojo pavadinimai ir adresai:

6.1. ŽIS valdytojas – Nacionalinė žemės tarnyba prie Žemės ūkio ministerijos, kurios adresas yra Gedimino pr. 19, LT-01103 Vilnius;

6.2. ŽIS tvarkytojas – valstybės įmonė Valstybės žemės fondas, kurios adresas yra Konstitucijos pr. 23A, LT-08105 Vilnius.

7. ŽIS valdytojas atsako už ŽIS saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir ŽIS duomenų tvarkymo teisėtumą bei atlieka šias funkcijas:

7.1. tvirtina ŽIS duomenų saugos politiką įgyvendinančius teisės aktus (toliau – ŽIS saugos dokumentai):

7.1.1. ŽIS saugaus elektroninės informacijos tvarkymo taisykles;

7.1.2. ŽIS veiklos tęstinumo valdymo planą;

7.1.3. ŽIS naudotojų administravimo taisykles;

7.1.4. ŽIS rizikos įvertinimo ataskaitą;

7.1.5. ŽIS rizikos įvertinimo ir rizikos valdymo priemonių planą;

7.1.6. ŽIS trūkumų šalinimo planą;

7.1.7. kitus teisės aktus.

7.2. kontroliuoja, kaip laikomasi Žemės informacinės sistemos nuostatuose (toliau – ŽIS nuostatai), ŽIS saugos dokumentuose ir kituose elektroninės informacijos saugą reglamentuojančiuose teisės aktuose nustatytų reikalavimų;

7.3. priima sprendimus dėl ŽIS techninių ir programinių priemonių, būtinų ŽIS duomenų saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

7.4. skiria saugos įgaliotinį ir administratorių;

7.5. priima sprendimą dėl ŽIS informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

7.6. atlieka kitas ŽIS nuostatais, šiais Saugos nuostatais ir kitais elektroninės informacijos saugą reglamentuojančiais teisės aktais jam priskirtas funkcijas.

8. ŽIS tvarkytojas atsako už ŽIS duomenų saugos įgyvendinimą, reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir kituose ŽIS saugos dokumentuose nustatyta tvarka bei:

8.1. pagal kompetenciją įgyvendina ŽIS nuostatų, Saugos nuostatų, ŽIS saugos dokumentų ir kitų elektroninės informacijos saugą reglamentuojančių teisės aktų reikalavimus;

8.2. užtikrina, kad ŽIS duomenys būtų apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio neteisėto veiksmo;

8.3. vykdo ŽIS techninę priežiūrą, užtikrina nepertraukiamą ŽIS veikimą, ŽIS duomenų saugą ir saugų ŽIS duomenų perdavimą kompiuterių tinklais;

8.4. teikia pasiūlymus ŽIS valdytojui dėl ŽIS duomenų saugos tobulinimo, ŽIS techninių ir programinių priemonių, būtinų ŽIS duomenų saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

8.5. atlieka ŽIS valdytojo vadovo pavestas ir ŽIS nuostatais, šiais Saugos nuostatais ir kitais ŽIS saugos dokumentais jam priskirtas funkcijas.

9. Saugos įgaliotinis įgyvendina ŽIS duomenų saugą ir atsako už ŽIS saugos dokumentų reikalavimų vykdymą bei atlieka šias funkcijas:

9.1. rengia ŽIS saugos dokumentų projektus (išskyrus ŽIS trūkumų šalinimo planą);

9.2. teikia ŽIS valdytojo vadovui pasiūlymus dėl:

9.2.1. administratorius skyrimo ir reikalavimų administratoriui nustatymo;

9.2.2. ŽIS saugos dokumentų priėmimo, keitimo ar panaikinimo;

9.2.3. ŽIS informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

9.3. koordinuoja elektroninės informacijos saugos incidentų, įvykusių ŽIS, tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais;

9.4. kasmet organizuoja ŽIS rizikos įvertinimą ir rengia ŽIS rizikos įvertinimo ataskaitą, o prireikus – ŽIS rizikos įvertinimo ir rizikos valdymo priemonių planą;

9.5. teikia administratoriui ir ŽIS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;

9.6. periodiškai inicijuoja administratoriaus ir ŽIS naudotojų mokymą ŽIS duomenų saugos klausimais, įvairiais būdais informuoja juos apie ŽIS duomenų saugos problematiką (priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės priimtiems naujiems darbuotojams ir pan.);

9.7. pasirašytinai supažindina administratorių ir ŽIS naudotojus su šiais Saugos nuostatais ir ŽIS saugos dokumentais ir atsakomybe, kylančia dėl jų pažeidimo;

9.8. atlieka ŽIS valdytojo vadovo pavestas bei šiais Saugos nuostatais ir kitais ŽIS saugos dokumentais jam priskirtas funkcijas.

10. Administratorius atsako už ŽIS infrastruktūros funkcionavimą ir ŽIS saugumą bei atlieka šias funkcijas:

10.1. vertina ŽIS naudotojų pasirengimą dirbti su ŽIS;

10.2. sukuria, keičia ir panaikina ŽIS naudotojų atitinkamas teises, jas administruoja;

10.3. vykdo ŽIS infrastruktūros (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, įsilaužimų aptikimo sistemų, duomenų perdavimo tinklų) ir ŽIS sudarančių posistemių priežiūrą;

10.4. nustato ŽIS pažeidžiamas vietas;

10.5. atlieka ŽIS saugumo reikalavimų atitikties vertinimą ir rengia ŽIS informacinių technologijų saugos atitikties vertinimo ataskaitą, o prireikus – ŽIS trūkumų šalinimo planą;

10.6. dalyvauja atliekant ŽIS rizikos įvertinimą ir rengiant ŽIS rizikos įvertinimo ataskaitą, o prireikus – ŽIS rizikos įvertinimo ir rizikos valdymo priemonių planą;

10.7. reguliariai, ne rečiau kaip kartą per metus ir (arba) po ŽIS pokyčio, patikrina (peržiūri) ŽIS sąranką ir ŽIS būsenos rodiklius.

10.8. parenka ŽIS techninės ir programinės įrangos saugos priemones bei nustato jų atitiktį ŽIS saugos dokumentų reikalavimams;

10.9. kontroliuoja, kad tvarkant ŽIS ir ŽIS duomenis nebūtų pažeisti Saugos nuostatų reikalavimai;

10.10. rengia pasiūlymus dėl ŽIS duomenų saugos ir ŽIS modernizavimo ir teikia juos saugos įgaliotiniui;

10.11. atlieka saugos įgaliotinio pavestas bei šiais Saugos nuostatais ir ŽIS saugos dokumentais jam priskirtas funkcijas.

11. ŽIS duomenų sauga užtikrinama vadovaujantis šiais teisės aktais:

11.1. Lietuvos Respublikos Valstybės informacinių išteklių valdymo įstatymu;

11.2. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716;

11.3. Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų saugos reikalavimais;

11.4. Lietuvos standartu LST ISO/IEC 27001:2013 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“;

11.5. Lietuvos standartu LST ISO/IEC 27002:2014 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“;

11.6. ŽIS nuostatais;

11.7. Saugos nuostatais ir kitais ŽIS saugos dokumentais.

II. ŽIS DUOMENŲ SAUGOS VALDYMAS

12. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ (toliau – Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas), 4.3 papunkčiu, ŽIS duomenys priskiriami žinybinės svarbos elektroninės informacijos kategorijai, kadangi dėl elektroninės informacijos saugumo pažeidimo gali kilti grėsmė įvykti procesams, kurie:

12.1. gali padaryti žalą vieno ar kelių fizinių ar juridinių asmenų teisėtiems interesams;

12.2. gali turėti neigiamų padarinių ŽIS tvarkytojo veiklai.

13. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 5.3 papunkčiu, ŽIS yra priskiriama trečios kategorijos informacinėms sistemoms, kadangi ŽIS apdorojama žinybinės svarbos elektroninė informacija.

14. Saugos įgaliotinis, atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacinės technologijos. Saugumo metodai“ grupės standartus, ne rečiau kaip vieną kartą per metus atlieka ŽIS rizikos įvertinimą, kurio metu išanalizuojami rizikos veiksniai, galimos jų pašalinimo arba neigiamo poveikio sumažinimo priemonės. Prireikus, saugos įgaliotinis gali atlikti neeilinį ŽIS rizikos įvertinimą.

15. Atlikęs ŽIS rizikos įvertinimą, saugos įgaliotinis parengia ŽIS rizikos įvertinimo ataskaitą. ŽIS rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos duomenų saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus ir rizikos priimtinumo kriterijus. Pagrindiniai rizikos veiksniai, kurie gali turėti įtakos ŽIS duomenų saugai, yra:

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

15.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis ŽIS duomenims gauti, ŽIS duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kt.);

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

16. Pagrindiniai elektroninės informacijos saugos valdymo priemonių parinkimo principai yra šie:

16.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

16.2. informacijos saugos priemonės diegimo kainos adekvatumas saugomos informacijos vertei;

16.3. turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

17. Atsižvelgdamas į ŽIS rizikos įvertinimo ataskaitą, saugos įgaliotinis prireikus, t. y. jeigu ŽIS rizikos įvertinimo ataskaitoje nustatyti rizikos veiksniai yra nepriimtini, parengia ŽIS rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti. ŽIS rizikos įvertinimo ataskaita, ŽIS rizikos įvertinimo ir rizikos valdymo priemonių planas teikiamas tvirtinti ŽIS valdytojo vadovui.

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

18. Saugos įgaliotinis ne rečiau kaip kartą per dvejus metus organizuoja ŽIS informacinių technologijų saugos reikalavimų atitikties vertinimą.

Atlikus ŽIS informacinių technologijų saugos atitikties vertinimą, administratorius rengia ŽIS informacinių technologijų saugos atitikties vertinimo ataskaitą, kuri pateikiama susipažinimui ŽIS valdytojo vadovui.

Jeigu atlikus ŽIS informacinių technologijų saugos atitikties vertinimą buvo nustatyta informacinių technologijų saugos neatitikčių 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“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas), nuostatoms, administratorius parengia ŽIS pastebėtų trūkumų šalinimo planą, kurį įsakymu tvirtina ŽIS valdytojo vadovas.

19. ŽIS informacinių technologijų saugos atitikties vertinimo ataskaitos, ŽIS trūkumų šalinimo plano kopijas ŽIS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

III. ŽIS ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

20. Priemonės ir metodai, kurie taikomi užtikrinant prieigą prie ŽIS, nurodant leistiną šios prieigos laiką ir būdą, nustatomi ŽIS naudotojų administravimo taisyklėse.

21. Taikomi šie ŽIS programinės įrangos naudojimo reikalavimai:

21.1. ŽIS tarnybinėse stotyse, ŽIS naudotojų kompiuteriuose diegiama tik legali ir saugi programinė įranga;

21.2. ŽIS tarnybinių stočių, ŽIS naudotojų kompiuterių operacinių sistemų ir taikomųjų programų struktūra sudaroma tokiu būdu, kad būtų užtikrintas didžiausias saugumo lygis (išjungiami nereikalingi darbui procesai ir reikmenys (angl. *services*), ribojamas priėjimas prie operacinės sistemos prievadų);

21.3. ŽIS tarnybinėse stotyse, ŽIS naudotojų kompiuteriuose privalo būti naudojama ir reguliariai ne rečiau kaip kartą per 10 dienų automatiškai atnaujinama programinė įranga, skirta apsaugai nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.);

21.4. ŽIS tarnybinėse stotyse neturi veikti programinė įranga, nesusijusi su ŽIS funkcine sistema;

21.5. ŽIS programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims, t. y. asmenims, nenurodytiems ŽIS naudotojų administravimo taisyklėse;

21.6. ŽIS naudotojų kompiuteriuose draudžiama naudoti programinę įrangą, nesusijusią su jų tiesiogine veikla ir funkcijomis;

21.7. Turi būti naudojama ŽIS administravimo programinės įrangos ugniasienė;

21.8. ŽIS funkcionuoti būtina programinė įranga (operacinės sistemos, duomenų bazių ir aplikacijų valdymo programinė įranga, interneto naršyklės, interneto naršyklių priedai ir kita) turi būti konfigūruojama laikantis programinės įrangos gamintojų saugaus konfigūravimo rekomendacijų. Programinės įrangos konfigūravimą atlieka administratorius;

21.9. ŽIS funkcionuoti būtina programinė įranga turi būti atnaujinama ne vėliau kaip per 5 darbo dienas nuo programinės įrangos gamintojų pranešimo apie programinės įrangos atnaujinimą gavimą dienos. Programinės įrangos atnaujinimą atlieka administratorius;

21.10. Programinės įrangos testavimas turi būti atliekamas naudojant atskirą tam skirtą testavimo aplinką. Programinės įrangos testavimą atlieka administratorius.

22. Kompiuterių tinklas, prie kurio prijungtos ŽIS tarnybinės stotys, nuo viešojo interneto turi būti atskirtas tinklo užkarda (angl. *firewall*), už šios tinklo užkardos priežiūrą atsako administratorius.

23. Prieiga prie ŽIS duomenų ŽIS naudotojams suteikiama pagal ŽIS naudotojų administravimo taisyklėse nustatytą tvarką ir sąlygas.

24. ŽIS duomenys automatiniu būdu į ŽIS teikiami ir (ar) per ŽIS gaunami tik pagal duomenų teikimo sutartyse nustatytą tvarką ir sąlygas, naudojant TCP/IP protokolą realiu laiku („on-line“ režimu) arba asinchroniniu režimu.

25. ŽIS naudotojams, savo tarnybinėms ar darbo funkcijoms vykdyti naudojantiems nešiojamuosius kompiuterius, ŽIS duomenims perduoti kompiuterių tinklais ne savo darbo vietoje turi būti naudojamas kompiuterio įjungimo slaptažodis ir papildomas ŽIS naudotojo tapatybės patvirtinimas.

26. ŽIS veiklos tęstinumui užtikrinti ŽIS duomenys yra periodiškai ne rečiau kaip kas 24 valandas kopijuojami į rezervinių kopijų laikmenas ir laikmenos saugomos taip, kad įvykus saugos incidentui visiškas ŽIS funkcionalumas ir veikla būtų atkurta per 8 valandas. Administratorius ne rečiau kaip kartą per metus atlieka rezervinių kopijų tinkamumo ir saugojimo kontrolę.

Rezervinių kopijų, pagal kurias būtų galima atstatyti ŽIS duomenis, darymo ir saugojimo tvarka nustatoma ŽIS saugaus elektroninės informacijos tvarkymo taisyklėse.

IV. REIKALAVIMAI PERSONALUI

27. Saugos įgaliotinis privalo išmanyti ŽIS duomenų saugos užtikrinimo principus, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, šiais Saugos nuostatais, ŽIS saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų informacijos tvarkymą informacinėje sistemoje, ir sugebėti prižiūrėti saugos politikos įgyvendinimą.

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

29. Administratorius turi išmanyti darbą su kompiuterių tinklais ir mokėti užtikrinti jų saugumą, būti susipažinęs su Saugos nuostatais ir ŽIS saugos dokumentais bei raštu sutikęs laikytis juose nustatytų reikalavimų. Administratorius privalo būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais, mokėti tvarkyti ŽIS duomenis.

30. ŽIS naudotojai privalo turėti darbo kompiuteriu įgūdžių, mokėti tvarkyti ŽIS duomenis, būti susipažinę su Saugos nuostatais ir ŽIS saugos dokumentais bei raštu sutikę laikytis juose nustatytų reikalavimų.

31. Saugos įgaliotinis ir ŽIS administratorius turi nuolat tobulinti kvalifikaciją duomenų saugos srityje. Saugos įgaliotinis ne rečiau kaip kartą per dvejus metus inicijuoja ŽIS naudotojų mokymą informacijos saugos klausimais, įvairiais būdais primena apie informacijos saugos problematiką (pvz., priminimai elektroniniu paštu, teminių seminarų organizavimas, atmintinės ir panašiai).

32. ŽIS naudotojai privalo rūpintis ŽIS ir joje tvarkomų duomenų saugumu.

33. ŽIS naudotojai, pastebėję saugos dokumentų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti administratoriui ir saugos įgaliotiniui.

34. Jeigu saugos įgaliotinis nebuvo informuotas apie Saugos nuostatų 33 punkte nurodytus pažeidimus, administratorius informuoja saugos įgaliotinį apie šiuos pažeidimus. Įtaręs neteisėtą

veiką, pažeidžiančią ar neišvengiamai pažeisiančią ŽIS saugą (jos konfidencialumą, vientisumą ar prieinamumą), saugos įgaliotinis apie tai turi pranešti ŽIS valdytojo vadovui ir kompetentingoms institucijoms, tiriančioms elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais.

35. ŽIS naudotojų veiksmus įvykus ŽIS duomenų saugos incidentui reglamentuoja bei ŽIS duomenų saugos incidentų tyrimo tvarką nustato ŽIS valdytojas ŽIS veiklos tęstinumo valdymo plane.

V. ADMINISTRATORIAUS IR ŽIS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

36. Administratorių ir ŽIS naudotojus su Saugos nuostatais ir ŽIS saugos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą pasirašytinai supažindina saugos įgaliotinis per 20 darbo dienų nuo šių dokumentų patvirtinimo. Saugos įgaliotinis tvarko ŽIS naudotojų supažindinimo su ŽIS saugos dokumentais žurnalą, kuriame pildomos šios skiltys: supažindinimo data, ŽIS naudotojo vardas ir pavardė, pareigos, parašas.

37. Saugos įgaliotinis informuoja administratorių ir ŽIS naudotojus apie Saugos nuostatų ar kitų saugos politiką įgyvendinančių teisės aktų pakeitimus. Informacija apie pasikeitimus saugos politiką reguliuojančiuose teisės aktuose siunčiama elektroniniu būdu. Pakartotinai su Saugos nuostatais ir ŽIS saugos dokumentais ŽIS naudotojai pasirašytinai supažindinami tik iš esmės pasikeitus Saugos nuostatams ir ŽIS saugos dokumentams.

VI. BAIGIAMOSIOS NUOSTATOS

38. Saugos nuostatai ir ŽIS saugos dokumentai turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per metus po ŽIS rizikos įvertinimo ar ŽIS informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo arba įvykus ŽIS valdytojo esminiams organizaciniams ar kitiems pokyčiams. Prireikus, Saugos nuostatai ir ŽIS saugos dokumentai turi būti tikslinami.

39. Saugos įgaliotinis, administratorius ir ŽIS naudotojai privalo saugoti ir neatskleisti ŽIS elektroninės informacijos, įsipareigojimas saugoti ir neatskleisti ŽIS elektroninės informacijos galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą.

40. Saugos įgaliotinis, administratorius, ŽIS naudotojai ir kiti asmenys, pažeidę Saugos nuostatus ir ŽIS saugos dokumentus, atsako įstatymų ir kitų teisės aktų nustatyta tvarka.

_____

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Nacionalinė žemės tarnyba prie Žemės ūkio ministerijos 188704927, Gedimino pr.19, Vilnius
Dokumento pavadinimas (antraštė)	Dėl Nacionalinės žemės tarnybos prie Žemės ūkio ministerijos direktoriaus 2011 m. lapkričio 22 d. įsakymo Nr. 1P-(1.3.)-267 „Dėl Žemės informacinės sistemos nuostatų ir Žemės informacinės sistemos duomenų saugos nuostatų patvirtinimo“ pakeitimo
Dokumento registracijos data ir numeris	2014-10-08 Nr. 1P-(1.3.)-390
Dokumento registracijos data ir numeris	2014-10-09 Nr. 2014-13929
Dokumento gavimo data ir dokumento gavimo registracijos numeris	2014-10-08 Nr. 13244
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	VAIDAS PAKALKA, Direktoriaus pavaduotojas
Sertifikatas išduotas	VAIDAS PAKALKA, Nacionalinė žemės tarnyba prie Žemės ūkio ministerijos LT
Parašo sukūrimo data ir laikas	2014-10-08 14:22:19
Parašo formatas	XAdES-X-L
Laiko žymoje nurodytas laikas	2014-10-08 18:43:06
Informacija apie sertifikavimo paslaugų teikėją	Nacionalinis sertifikavimo centras (IssuingCA-A), Gyventoju registro tarnyba prie LR VRM - i.k. 188756767 LT
Sertifikato galiojimo laikas	2013-12-20 - 2016-12-19
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	"Gauto dokumento registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "SSC GDL NH CA, Skaitmeninio sertifikavimo centras LT" išduotą sertifikatą "TEISĖS AKTŲ REGISTRAS, Lietuvos Respublikos Seimo kanceliarija LT", sertifikatas galioja nuo 2013-12-31 iki 2014-12-31 "Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "SSC GDL NH CA, Skaitmeninio sertifikavimo centras LT" išduotą sertifikatą "TEISĖS AKTŲ REGISTRAS, Lietuvos Respublikos Seimo kanceliarija LT", sertifikatas galioja nuo 2013-12-31 iki 2014-12-31
Pagrindinio dokumento priedų skaičius	1
Pagrindinio dokumento pridedamų dokumentų skaičius	-
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Signa 2010 (1.2.0.v20130701-5042)
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja (2014-10-10)
Paieškos nuoroda	https://www.e-tar.lt/portal/legalAct.html?documentId=8a25ffa04ff711e485f39f55fd139d01
Papildomi metaduomenys	Nuorašą suformavo 2014-10-10 00:02:34 TAIS