

Neoficialus įsakymo tekstas
Neskelbtas „Valstybės žiniuose“

LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO MINISTRO
Į S A K Y M A S

**DĖL LIETUVOS RESPUBLIKOS ŪKININKŲ ŪKIŲ REGISTRO DUOMENŲ
SAUGOS NUOSTATŲ PATVIRTINIMO**

2007 m. kovo 22 d. Nr. 3D-128
Vilnius

Nauja įsakymo redakcija
Galioja nuo 2013 m. sausio 16 d.
Nr. [3D-24](#), 2013-01-11, Žin., 2013, Nr. 5-192 (2013-01-15)

LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO MINISTRO
Į S A K Y M A S

**DĖL LIETUVOS RESPUBLIKOS ŪKININKŲ ŪKIŲ REGISTRO DUOMENŲ
SAUGOS NUOSTATŲ PATVIRTINIMO**

2013 m. sausio 11 d. Nr. 3D-24
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų, patvirtintų Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. [83-2075](#); 2007, Nr. [49-1891](#); 2008, Nr. [85-3393](#)), 6.1 ir 8 punktais, Valstybės informacinių sistemų steigimo ir įteisinimo taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 2004 m. balandžio 19 d. nutarimu Nr. 451 (Žin., 2004, Nr. [58-2061](#); 2007, Nr. [110-4506](#)), 6 punktu:

1. T v i r t i n u Lietuvos Respublikos ūkininkų ūkių registro duomenų saugos nuostatus (pridedama).

2. P a v e d u:

2.1. Žemės ūkio informacinių sistemų skyriui ne vėliau kaip per 6 mėnesius nuo šio įsakymo įsigaliojimo datos parengti saugos politiką įgyvendinančių dokumentų projektus ir suderinti su Lietuvos Respublikos vidaus reikalų ministerija.

2.2. Valstybės įmonei Žemės ūkio informacijos ir kaimo verslo centrui per 14 darbo dienų nuo šio įsakymo įsigaliojimo datos paskirti Lietuvos Respublikos ūkininkų ūkių registro duomenų saugos įgaliotinį.

ŽEMĖS ŪKIO MINISTRAS

VIGILIJUS JUKNA

SUDERINTA

Lietuvos Respublikos vidaus reikalų ministerijos
2013 m. sausio 3 d. raštu Nr. 1D-73(52)

Nauja nuostatų redakcija
Galioja nuo 2013 m. sausio 16 d.
Nr. [3D-24](#), 2013-01-11, Žin., 2013, Nr. 5-192 (2013-01-15)

PATVIRTINTA
Lietuvos Respublikos žemės
ūkio ministro
2007 m. kovo 22 d. įsakymu
Nr. 3D-128
(Lietuvos Respublikos žemės
ūkio ministro 2013 m. sausio
11 d. įsakymo Nr. 3D-24
redakcija)

LIETUVOS RESPUBLIKOS ŪKININKŲ ŪKIŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos ūkininkų ūkių registro duomenų saugos nuostatai (toliau – saugos nuostatai) reglamentuoja Ūkininkų ūkių registro (toliau – ŪŪR) saugos politiką. Saugos politiką įgyvendina ŪŪR saugaus elektroninės informacijos tvarkymo taisyklės, ŪŪR veiklos tęstinumo valdymo planas, ŪŪR naudotojų administravimo taisyklės, kurias tvirtina ŪŪR tvarkytojas.

2. Šiuose saugos nuostatuose vartojama sąvoka **ŪŪR naudotojas** – valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, turintis teisę naudotis ŪŪR ištekliais numatytiems funkcijoms atlikti.

Kitos šiuose saugos nuostatuose vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme (Žin., 2011, Nr. [163-7739](#)), Bendruosiuose elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuose, patvirtintuose Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. [83-2075](#); 2007, Nr. [49-1891](#)), Saugos dokumentų turinio gairėse, patvirtintose Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. [53-2070](#)), Valstybės informacinių sistemų steigimo ir įteisinimo taisyklėse, patvirtintose Lietuvos Respublikos Vyriausybės 2004 m. balandžio 19 d. nutarimu Nr. 451 (Žin., 2004, Nr. [58-2061](#)), kituose teisės aktuose ir Lietuvos Respublikos standartuose LST ISO/IEC 27002:2009 ir LST ISO/IEC 27001:2006.

3. ŪŪR tvarkomos elektroninės informacijos saugumo tikslas – sudaryti sąlygas saugiai automatizuotu būdu saugoti ir tvarkyti ŪŪR duomenis, užtikrinti duomenų konfidencialumą, vientisumą ir prieinamumą.

4. Esama ŪŪR duomenų saugos būklė nustatoma kasmetinio rizikos vertinimo metu ir fiksuojama rizikos įvertinimo ataskaitoje.

5. Elektroninės ŪŪR duomenų saugos užtikrinimo prioritetinės kryptys:

- 5.1. ŪŪR duomenų konfidencialumo užtikrinimas;
- 5.2. ŪŪR reikalaujamo prieinamumo lygio užtikrinimas;
- 5.3. prieigos prie ŪŪR kontrolė;
- 5.4. ŪŪR naudotojų mokymas.
6. Saugos nuostatai taikomi:
 - 6.1. ŪŪR valdytojui – Lietuvos Respublikos žemės ūkio ministerijai, Gedimino per. 19, LT-01103 Vilnius;
 - 6.2. ŪŪR tvarkytojui – valstybės įmonei Žemės ūkio informacijos ir kaimo verslo centrui, V. K. Kudirkos g. 18-1, LT-03105 Vilnius;
 - 6.3. ŪŪR naudotojams;
 - 6.4. ŪŪR administratoriui;
 - 6.5. ŪŪR saugos įgaliotiniui.
7. ŪŪR valdytojo funkcijos ir atsakomybė:
 - 7.1. rengia ir priima teisės aktus, užtikrinančius ŪŪR duomenų tvarkymo teisėtumą ir ŪŪR duomenų saugą, atlieka jų nuostatų laikymosi priežiūrą;
 - 7.2. analizuoja gaunamus pasiūlymus dėl ŪŪR duomenų saugos, juos apibendrina ir priima sprendimus dėl ŪŪR tobulinimo;
 - 7.3. vadovauja ŪŪR tvarkytojo veiklai, kuriant ir diegiant ŪŪR, taip pat užtikrina ŪŪR veikimą, tobulinimą ir duomenų saugą;
 - 7.4. priima sprendimus dėl ŪŪR rizikos veiksnių vertinimo atlikimo;
 - 7.5. atlieka kitas saugos nuostatų, ŪŪR nuostatų ir kitų teisės aktų nustatytas funkcijas;
 - 7.6. pagal kompetenciją atsako už informacijos saugą;
 - 7.7. paveda ŪŪR tvarkytojui skirti ŪŪR saugos įgaliotinį.
8. ŪŪR tvarkytojo funkcijos ir atsakomybė:
 - 8.1. užtikrina ŪŪR prieinamumą;
 - 8.2. pagal kompetenciją atsako už informacijos saugą, užtikrina ŪŪR taikomajai programinei įrangai, tarnybinėms stotims ir jose esantiems duomenims funkcionuoti būtinos informacinių technologijų infrastruktūros (toliau – serverių sritis) saugą;
 - 8.3. rengia ir saugo serverių srities saugai užtikrinti būtiną dokumentaciją;
 - 8.4. sudaro ŪŪR duomenų gavimo ir teikimo sutartis;
 - 8.5. ŪŪR valdytojo raštišku pavedimu skiria ŪŪR saugos įgaliotinį;
 - 8.6. ŪŪR valdytojo raštišku pavedimu skiria ŪŪR administratorių;
 - 8.7. atlieka kitas saugos nuostatų, ŪŪR nuostatų ir kitų teisės aktų nustatytas funkcijas.
9. ŪŪR saugos įgaliotinio funkcijos ir atsakomybė:
 - 9.1. teikia ŪŪR tvarkytojo vadovui pasiūlymus dėl:
 - 9.1.1. ŪŪR administratoriaus paskyrimo;
 - 9.1.2. ŪŪR saugos dokumentų priėmimo, keitimo arba panaikinimo;
 - 9.1.3. informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;
 - 9.2. koordinuoja elektroninės informacijos saugos incidentų, įvykusių ŪŪR, tyrimą;
 - 9.3. teikia ŪŪR administratoriui privalomus vykdyti nurodymus ir pavedimus;
 - 9.4. ŪŪR tvarkytojo nustatyta tvarka supažindina ŪŪR administratorių ir ŪŪR naudotojus su saugos nuostatais, saugos dokumentų reikalavimais ir jų atsakomybe už reikalavimų nesilaikymą bei teisės aktais, nurodytais saugos nuostatų 12 punkte, kuriais vadovaujamosi tvarkant elektroninę informaciją užtikrinant jos saugumą;

- 9.5. atsako už ŪŪR elektroninės informacijos saugos įgyvendinimą;
- 9.6. atsako už ŪŪR rizikos vertinimo atlikimo organizavimą, rizikos įvertinimo ir rizikos valdymo priemonių plano parengimą;
- 9.7. atsako už ŪŪR informacinių technologijų saugos atitikties vertinimo organizavimą;
- 9.8. atlieka kitas ŪŪR valdytojo vadovo pavestas, šiais saugos nuostatais bei kitais teisės aktais jam priskirtas funkcijas.
10. ŪŪR administratoriaus funkcijos ir atsakomybė:
- 10.1. užtikrina ŪŪR serverių srities funkcionavimą ir prieigų prie ŪŪR infrastruktūros išteklių teisių suteikimą;
- 10.2. užtikrina ŪŪR sudarančių komponentų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų, ugniasienių, įsilaužimų aptikimo sistemų, duomenų perdavimo tinklų) sąranką, kuri atitiktų ŪŪR saugos dokumentų reikalavimus;
- 10.3. pagal kompetenciją teikia pasiūlymus dėl ŪŪR palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;
- 10.4. informuoja ŪŪR saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikia pasiūlymus dėl elektroninės informacijos saugos incidentų pašalinimo;
- 10.5. atsako už atsarginių ŪŪR duomenų kopijų darymo, atkūrimo ir už ŪŪR taikomosios programinės įrangos (aplikacijų) kopijų darymo organizavimą ir peržiūrą;
- 10.6. atlieka ŪŪR priežiūrą.
11. ŪŪR naudotojų funkcijos:
- 11.1. rūpintis ŪŪR ir joje tvarkomos informacijos saugumu;
- 11.2. tvarkyti ir naudoti ŪŪR duomenis, vykdant tiesiogines su darbu susijusias funkcijas;
- 11.3. atlikti kitas saugos nuostatų, ŪŪR nuostatų ir kitų teisės aktų nustatytas funkcijas.
12. Teisės aktai, kuriais vadovaujamosi tvarkant ŪŪR, tvarkomi duomenys ir užtikrinama sauga:
- 12.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (Žin., 1996, Nr. [63-1479](#); 2008, Nr. [22-804](#));
- 12.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas (Žin., 1996, Nr. [63-1479](#); 2008, Nr. [22-804](#));
- 12.3. Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai, patvirtinti Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. [83-2075](#); 2007, Nr. [49-1891](#));
- 12.4. Valstybės informacinių sistemų steigimo ir įteisinimo taisyklės, patvirtintos Lietuvos Respublikos Vyriausybės 2004 m. balandžio 19 d. nutarimu Nr. 451 (Žin., 2004, Nr. [58-2061](#));
- 12.5. Saugos dokumentų turinio gairės, patvirtintos Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. [53-2070](#));
- 12.6. Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės, patvirtintos Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymu Nr. 1V-247 (Žin., 2007, Nr. [78-3160](#); 2008, Nr. [127-4866](#)) (toliau – Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės);

12.7. Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai, patvirtinti Lietuvos Respublikos vidaus reikalų ministro 2008 m. spalio 27 d. įsakymu Nr. 1V-384 (Žin., 2008, Nr. [127-4866](#));

12.8. Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtinti Valstybės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71 (1.12) (Žin., 2008, Nr. [135-5298](#)) (toliau – Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms);

12.9. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 (Žin., 2004, Nr. [80-2855](#));

12.10. Lietuvos standartai LST ISO/IEC 27002:2009 ir LST ISO/IEC 27001:2006 ir kiti Lietuvos ir tarptautiniai standartai, reglamentuojantys informacijos saugumą;

12.11. kiti teisės aktai, reglamentuojantys elektroninės informacijos apsaugą valstybės institucijose.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

13. ŪŪR elektroninės informacijos priskyrimo atitinkamai kategorijai bendrieji reikalavimai:

13.1. Vadovaujantis Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairių 3.3.2 punktu, dėl ŪŪG tvarkomų asmens duomenų informacinė sistema yra priskiriama trečios kategorijos informacinėms sistemoms;

13.2. Vadovaujantis Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms 7.2 punktu, dėl galimybės per išorinius duomenų perdavimo tinklus tvarkyti ŽŪKVR saugomus asmens duomenis ŽŪKVR priskiriamas antrasis saugumo lygis.

14. Pagrindinės nuostatos dėl rizikos veiksnių vertinimo:

14.1. ŪŪR rizikos vertinimą inicijuoja ŪŪR valdytojas;

14.2. ŪŪR informacinės saugos rizika nustatoma periodinio rizikos vertinimo metu;

14.3. ŪŪR rizikos vertinimas atliekamas ne rečiau kaip kartą per metus.

14.4. Vertinimo metu:

14.4.1. įvertinama saugos nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų atitiktis esamai ŪŪR duomenų saugos situacijai;

14.4.2. inventorizuojama ŪŪR techninė ir programinė įranga;

14.4.3. patikrinamos visose tarnybinėse stotyse įdiegtos programos ir jų sąranka;

14.5. ŪŪR rizikos veiksniai vertinami taikant kokybinę rizikos vertinimo metodiką;

14.6. ŪŪR vertinimas atliekamas vadovaujantis:

14.6.1. Lietuvos Respublikos duomenų saugą reglamentuojančiais teisės aktų reikalavimais;

14.6.2. Lietuvos ir tarptautiniuose grupės standartuose „Informacijos technologija. Saugumo technika“ pateikiamomis rekomendacijomis;

14.7. ŪŪR rizikos įvertinimas išdėstomas rizikos įvertinimo ataskaitoje. ŪŪR rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos ŪŪR informacijos saugai. Svarbiausi rizikos veiksniai:

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

14.7.2. subjektyvūs tyčiniai (nesankcionuotas naudojimas ŪŪR duomenims gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymas, saugos pažeidimai, vagystės ir kita);

14.7.3. nenugalima jėga (*force majeure*);

14.8. ŪŪR valdytojas, atsižvelgdamas į ŪŪR rizikos įvertinimo ataskaitą, prireikus tvirtina ŪŪR saugos įgaliotinio parengtą rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

15. Siekiant užtikrinti saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose išdėstytų nuostatų įgyvendinimo kontrolę, ŪŪR saugos įgaliotinis ne rečiau kaip kartą per 2 metus organizuoja ŪŪR informacinių technologijų saugos atitikties vertinimą, kurio metu:

15.1. įvertinama saugos nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų atitiktis realiai ŪŪR duomenų saugos situacijai;

15.2. inventorizuojama ŪŪR techninė ir programinė įranga;

15.3. patikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų ŪŪR naudotojų kompiuterinių darbo vietų, visose tarnybinėse stotyse įdiegtos programos ir jų sąranka;

15.4. patikrinama ŪŪR naudotojams suteiktų teisių ir vykdomų funkcijų atitiktis;

15.5. įvertinamas pasirengimas užtikrinti ŪŪR veiklos tęstinumą įvykus saugos incidentui;

15.6. ŪŪR valdytojas, atsižvelgdamas į ŪŪR informacinių technologijų saugos reikalavimų atitikties vertinimo rezultatus, prireikus tvirtina ŪŪR saugos įgaliotinio parengtą pastebėtų trūkumų šalinimo planą, kuriame nurodomi atsakingi vykdytojai ir nustatomi numatytų priemonių įgyvendinimo terminai.

16. ŪŪR saugos priemonės parenkamos įvertinus galimus ŪŪR duomenų vientisumo, konfidencialumo ir prieinamumo rizikos veiksnius.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

17. Metodai ir priemonės, kurie taikomi užtikrinant prieigą prie ŪŪR:

17.1. prieigos prie ŪŪR teisės suteikia ŪŪR administratorius. Pasikeitus ŪŪR naudotojo pareigoms ar atliekamoms užduotims, suteikta prieiga prie ŪŪR turi būti nedelsiant užblokuojama. ŪŪR naudotojams suteiktos prieigos teisės periodiškai, bet ne rečiau kaip kartą per metus, turi būti peržiūrimos, siekiant nustatyti ir pašalinti subjektus, kuriems prieigos teisės prie ŪŪR turi būti panaikintos arba pakeistos. Už periodinę ŪŪR naudotojų teisių peržiūrą atsakingas ŪŪR saugos įgaliotinis;

17.2. prieš suteikiant prieigą, ŪŪR administratorius privalo įsitikinti, kad ŪŪR naudotojas yra susipažinęs su informacijos saugos dokumentais bei žino savo atsakomybę tvarkant ar naudojant ŪŪR duomenis;

17.3. kiekvienas ŪŪR naudotojas sistemoje turi būti unikaliai atpažįstamas pagal jam suteiktą atpažinties kodą ir atitinkamą slaptažodį;

17.4. ŪŪR naudotojų prieigai prie ŪŪR naudojamas šifruotas HTTPS duomenų perdavimo protokolas bei interneto naršyklė.

18. ŪŪR tarnybinėse stotyse privalo būti naudojama programinė įranga, skirta kovai su kenksminga programine įranga, atnaujinama automatiniu būdu ne rečiau kaip kas 5 (penkias) darbo dienas. Pagrindinės programinės įrangos, skirtos apsaugoti ŪŪR nuo kenksmingos programinės įrangos, naudojimo nuostatos:

18.1. ŪŪR funkcionuoti būtina programinė tarnybinių stočių ir ŪŪR naudotojų kompiuteriuose esanti programinė įranga (operacinės sistemos, duomenų bazių ir aplikacijų valdymo programinė įranga, interneto naršyklės, interneto naršyklių priedai ir kt.) turi būti konfigūruojama laikantis programinės įrangos gamintojų saugaus konfigūravimo rekomendacijų. Už tarnybinių stočių programinės įrangos kontrolę atsakingas ŪŪR administratorius;

18.2. ŪŪR funkcionuoti būtina serverių srities ir ŪŪR naudotojų kompiuteriuose esanti programinė įranga turi būti atnaujinama ne vėliau kaip per 5 (penkias) darbo dienas po programinės įrangos gamintojų pranešimo apie programinės įrangos atnaujinimą. Už atnaujinimų atlikimo kontrolę atsakingas ŪŪR administratorius;

18.3. ŪŪR naudotojų kompiuteriuose prieigos teisės turi būti apribojamos iki minimalių, būtinų darbo užduotims atlikti teisių;

18.4. ŪŪR naudotojų kompiuteriai turi būti apsaugoti lokaliomis ugniasienėmis;

18.5. ŪŪR naudotojų kompiuteriuose turi būti naudojama antivirusinė programinė įranga, apsauganti nuo kenksmingų programų, įskaitant elektroninio pašto apsaugą. Antivirusinė programinė įranga periodiškai, ne rečiau kaip kartą per savaitę, turi būti automatiškai atnaujinama.

19. Programinės įrangos naudojimo ribojimo nuostatos:

19.1. ŪŪR tarnybinėse stotyse neturi veikti programinė įranga, nesusijusi su ŪŪR duomenų tvarkymu, ŪŪR naudotojų ir pačios įrangos administravimu.

20. Kompiuterių tinklo filtravimo įrangos naudojimo nuostatos:

20.1. ŪŪR elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų telekomunikacijos tinklų naudojant užkardą;

20.2. konfigūruojant ŪŪR elektroninės informacijos perdavimo tinklo užkardas turi būti naudojami tik organizacijos veiklai būtini tinklo protokolai ir užkardų prievadai;

20.3. ŪŪR administratorius organizuoja ŪŪR serverių srities tinklo užkardų administravimą, priežiūrą, operacinės sistemos atnaujinimą ir saugią užkardų konfigūraciją;

20.4. ŪŪR serverių srities tinklo užkardų konfigūracijos aprašymas (užkardos taisyklės) saugomas ŪŪR saugos įgaliotinio. Užkardų konfigūracija peržiūrima ne rečiau kaip kartą per metus. Peržiūrą inicijuoja ŪŪR saugos įgaliotinis.

21. Leistinos kompiuterių (įskaitant nešiojamuosius) naudojimo ribos:

21.1. stacionarieji ir nešiojamieji ŪŪR naudotojų kompiuteriai privalo būti naudojami tik su tiesioginių pareigų atlikimu susijusiai veiklai atlikti. Iš kompiuterių, kurie perduodami remontuoti ar techninei priežiūrai atlikti, turi būti pašalinta visa riboto naudojimo ŪŪR elektroninė informacija;

21.2. visiems ŪŪR naudotojų naudojamiems kompiuteriams privaloma naudoti papildomas saugos priemones, kuriomis patvirtinama kompiuterio naudotojo tapatybė bei šifruojami riboto naudojimo duomenys.

22. Metodai, kurie leidžiami užtikrinant saugų ŪŪR elektroninės informacijos teikimą ir (ar) gavimą:

22.1. ŪŪR duomenys perduodami automatinio būdu TCP/IP protokolu realiu laiku arba asinchroniniu režimu pagal ŪŪR duomenų teikimo ir gavimo sutartis, kuriose nustatytos perduodamų duomenų specifikacijos, perdavimo sąlygos ir tvarka;

22.2. už duomenų teikimo ir gavimo sutartyse nurodomų saugos reikalavimų identifikavimą, suformulavimą ir įgyvendinimo organizavimą atsakingas ŪŪR saugos įgaliotinis.

23. Pagrindiniai atsarginių ŪŪR duomenų kopijų darymo ir atkūrimo reikalavimai:

23.1. atsarginių ŪŪR duomenų kopijų darymas ir atkūrimas turi būti atliekamas laikantis Lietuvos Respublikos teisės aktų nustatytų reikalavimų;

23.2. atsarginės ŪŪR duomenų kopijos turi būti daromos ir jų atkūrimas turi būti atliekamas pagal ŪŪR tvarkytojo svarbiausios veiklos atsarginių kopijų administravimo procedūros aprašą, patvirtintą ŪŪR tvarkytojo generalinio direktoriaus;

23.3. už atsarginių ŪŪR duomenų kopijų darymo ir atkūrimo bei už ŪŪR taikomosios programinės įrangos (aplikacijų) kopijų darymo organizavimą ir peržiūrą yra atsakingas ŪŪR saugos įgaliotinis.

IV. REIKALAVIMAI PERSONALUI

24. ŪŪR saugos įgaliotinis privalo išmanyti informacijos saugos užtikrinimo principus, savo darbe vadovautis saugos dokumentais bei kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų duomenų tvarkymą, standartais ir kitais dokumentais, sugebėti prižiūrėti, kaip įgyvendinama ŪŪR saugos politika.

25. ŪŪR administratorius privalo išmanyti ŪŪR informacijos saugos politikos principus, darbą su duomenų perdavimo tinklais, mokėti užtikrinti jų saugą, taip pat administruoti ir prižiūrėti informacines sistemas, turi būti susipažinęs su šiais saugos nuostatais ir kitais susijusiais saugos dokumentais.

26. ŪŪR naudotojai turi turėti naudojimosi kompiuteriu įgūdžių, būti susipažinę su šiais saugos nuostatais ir kitais susijusiais saugos dokumentais.

27. ŪŪR naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veikos požymių ar netinkamai veikiančių ŪŪR duomenų saugos užtikrinimo priemonių, nedelsdami privalo apie tai pranešti ŪŪR administratoriui.

28. ŪŪR administratorius apie saugos nuostatų 27 punkte nurodytus pažeidimus informuoja ŪŪR saugos įgaliotinį. Įtaręs neteisėtą veiklą, pažeidžiančią ar neišvengiamai pažeisiančią ŪŪR saugą (jos konfidencialumą, vientisumą ar prieinamumą), ŪŪR saugos įgaliotinis apie tai turi pranešti kompetentingoms institucijoms.

29. Visi ŪŪR naudotojai privalo būti supažindinti su ŪŪR saugos dokumentais, savo pareigomis ir atsakomybe, susijusia su ŪŪR elektroninės informacijos sauga, bei teisės aktais, kuriais vadovaujamas tvarkant elektroninę informaciją, užtikrinant jos saugumą.

30. Už ŪŪR naudotojų supažindinimą su ŪŪR saugos dokumentais, saugos nuostatų 12 punkte nurodytais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, taip pat su atsakomybe už saugos dokumentų nuostatų pažeidimus atsakingas ŪŪR saugos įgaliotinis.

V. BAIGIAMOSIOS NUOSTATOS

31. Asmenys, pažeidę šių saugos nuostatų ir kitų duomenų saugos politiką įgyvendinančių teisės aktų nuostatas, atsako įstatymų nustatyta tvarka.

Pakeitimai:

1.

Lietuvos Respublikos žemės ūkio ministerija, Įsakymas

Nr. [3D-24](#), 2013-01-11, Žin., 2013, Nr. 5-192 (2013-01-15)

DĖL LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO MINISTRO 2007 M. KOVO 22 D. ĮSAKYMO NR. 3D-128 "DĖL LIETUVOS RESPUBLIKOS ŪKININKŲ ŪKIŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO" PAKEITIMO

*** Pabaiga ***

Redagavo Vyriausioji specialistė Laimutė Aleksejevienė (2013-02-11)

Tel. (8 5) 239 1056