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

DĖL LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO IR KAIMO VERSLO REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2013 m. sausio 11 d. Nr. 3D-22
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 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 žemės ūkio ir kaimo verslo 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 Žemės ūkio ir kaimo verslo registro saugaus elektroninės informacijos tvarkymo taisyklių, Žemės ūkio ir kaimo verslo registro veiklos tęstinumo valdymo plano ir Žemės ūkio ir kaimo verslo registro naudotojų administravimo taisyklių projektus ir suderinti juos su Lietuvos Respublikos vidaus reikalų ministerija.

2.2. Valstybės įmonei Žemės ūkio informacijos ir kaimo verslo centui per 14 darbo dienų nuo šio įsakymo įsigaliojimo datos paskirti Lietuvos Respublikos žemės ūkio ir kaimo verslo 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)

PATVIRTINTA
Lietuvos Respublikos žemės ūkio ministro
2013 m. sausio 11 d. įsakymu Nr. 3D-22

LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO IR KAIMO VERSLO REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos žemės ūkio ir kaimo verslo registro duomenų saugos nuostatai (toliau – saugos nuostatai) reglamentuoja Lietuvos Respublikos žemės ūkio ir kaimo verslo registro (toliau – ŽŪKVR) duomenų saugos politiką.

2. Šiuose saugos nuostatuose vartojama sąvoka **ŽŪKVR naudotojas** – valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, turintis teisę naudotis ŽŪKVR ištekliais saugos nuostatų 11 punkte numatytoms 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. ŽŪKVR tvarkomos elektroninės informacijos saugumo tikslas – sudaryti sąlygas saugiai automatizuotu būdu saugoti ir tvarkyti ŽŪKVR duomenis, užtikrinti duomenų konfidencialumą, vientisumą ir prieinamumą.

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

5. Elektroninės ŽŪKVR duomenų saugos užtikrinimo prioritetinės kryptys:

5.1. ŽŪKVR duomenų konfidencialumo užtikrinimas;

5.2. ŽŪKVR reikalaujamo prieinamumo lygio užtikrinimas;

5.3. prieigos prie ŽŪKVR kontrolė;

5.4. ŽŪKVR naudotojų mokymas.

6. Saugos nuostatai taikomi:

6.1. ŽŪKVR valdytojui – Lietuvos Respublikos žemės ūkio ministerijai, Gedimino pr. 19, LT-01103 Vilnius;

6.2. ŽŪKVR tvarkytojui – valstybės įmonei Žemės ūkio informacijos ir kaimo verslo centrui, V. Kudirkos g. 18-1, LT-03105 Vilnius;

6.3. ŽŪKVR naudotojams;

6.4. ŽŪKVR administratoriui;

6.5. ŽŪKVR saugos įgaliotiniui.

7. ŽŪKVR valdytojo funkcijos ir atsakomybė:

7.1. rengia ir priima teisės aktus, užtikrinančius ŽŪKVR duomenų tvarkymo teisėtumą ir ŽŪKVR duomenų saugą, atlieka saugos nuostatų laikymosi priežiūrą;

7.2. analizuoja gaunamus pasiūlymus dėl ŽŪKVR duomenų saugos, juos apibendrina ir priima sprendimus dėl ŽŪKVR tobulinimo;

7.3. vadovauja ŽŪKVR tvarkytojo veiklai, kuriant ir diegiant ŽŪKVR, taip pat užtikrina ŽŪKVR veikimą, tobulinimą ir duomenų saugą;

7.4. priima sprendimus dėl ŽŪKVR rizikos veiksnių vertinimo atlikimo;

7.5. atlieka kitas saugos nuostatų, Lietuvos Respublikos Žemės ūkio ir kaimo verslo

registro nuostatų, patvirtintų Lietuvos Respublikos Vyriausybės 2002 m. rugpjūčio 27 d. nutarimu Nr. 1351 (Žin., 2002, Nr. 84-3645; 2011, Nr. 230) (toliau – ŽŪKVR nuostatai) ir kitų teisės aktų nustatytas funkcijas;

7.6. pagal kompetenciją atsako už informacijos saugą;

7.7. paveda ŽŪKVR tvarkytojui skirti ŽŪKVR saugos įgaliotinį.

8. ŽŪKVR tvarkytojo funkcijos ir atsakomybė:

8.1. užtikrina ŽŪKVR prieinamumą;

8.2. pagal kompetenciją atsako už informacijos saugą, užtikrina ŽŪKVR 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 ŽŪKVR duomenų gavimo ir teikimo sutartis;

8.5. ŽŪKVR valdytojo raštišku pavedimu skiria ŽŪKVR saugos įgaliotinį;

8.6. ŽŪKVR valdytojo raštišku pavedimu skiria ŽŪKVR administratorių;

8.7. atlieka kitas saugos nuostatų, ŽŪKVR nuostatų ir kitų teisės aktų nustatytas funkcijas.

9. ŽŪKVR saugos įgaliotinio funkcijos ir atsakomybė:

9.1. teikia ŽŪKVR tvarkytojo vadovui pasiūlymus dėl:

9.1.1. ŽŪKVR administratoriaus paskyrimo;

9.1.2. ŽŪKVR saugos dokumentų priėmimo, keitimo arba panaikinimo;

9.1.3. informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

9.2. koordinuoja elektroninės informacijos saugos incidentų, įvykusių ŽŪKVR, tyrimą;

9.3. teikia ŽŪKVR administratoriui privalomus vykdyti nurodymus ir pavedimus;

9.4. supažindina ŽŪKVR administratorių ir ŽŪKVR naudotojus su saugos nuostatais, saugos dokumentų reikalavimais ir jų atsakomybe už reikalavimų nesilaikymą bei teisės aktais, nurodytais saugos nuostatų 12 punkte, kuriais vadovaujamasi tvarkant elektroninę informaciją užtikrinant jos saugumą;

9.5. atsako už ŽŪKVR elektroninės informacijos saugos įgyvendinimą;

9.6. atsako už ŽŪKVR rizikos vertinimo atlikimo organizavimą, rizikos įvertinimo ir rizikos valdymo priemonių plano parengimą;

9.7. atsako už ŽŪKVR informacinių technologijų saugos atitikties vertinimo organizavimą;

9.8. atlieka kitas ŽŪKVR valdytojo vadovo pavestas, šiais saugos nuostatais bei kitais teisės aktais jam priskirtas funkcijas.

10. ŽŪKVR administratoriaus funkcijos ir atsakomybė:

10.1. užtikrina ŽŪKVR serverių srities funkcionavimą ir prieigų prie ŽŪKVR infrastruktūros išteklių teisių suteikimą;

10.2. užtikrina ŽŪKVR sudarančių komponentų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų, ugniasienių, įsilaužimų aptikimo sistemų, duomenų perdavimo tinklų) sąranką, kuri atitiktų ŽŪKVR saugos dokumentų reikalavimus;

10.3. pagal kompetenciją teikia pasiūlymus dėl ŽŪKVR palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

10.4. informuoja ŽŪKVR saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikia pasiūlymus dėl elektroninės informacijos saugos incidentų pašalinimo;

10.5. atsako už atsarginių ŽŪKVR duomenų kopijų darymo, atkūrimo ir už ŽŪKVR taikomosios programinės įrangos (aplikacijų) kopijų darymo organizavimą ir peržiūrą;

10.6. atlieka ŽŪKVR priežiūrą.

11. ŽŪKVR naudotojų funkcijos:

11.1. rūpintis ŽŪKVR ir joje tvarkomos informacijos saugumu;

11.2. tvarkyti ir naudoti ŽŪKVR duomenis, vykdant tiesiogines su darbu susijusias

funkcijas;

11.3. atlikti kitas saugos nuostatų, ŽŪKVR nuostatų ir kitų teisės aktų nustatytas funkcijas.

12. Teisės aktai, kuriais vadovaujantis tvarkomas ŽŪKVR, 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., 2011, Nr. 163-7739);

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, nustatantys saugų informacinės sistemos duomenų tvarkymą;

12.11. kiti teisės aktai, reglamentuojantys elektroninės informacijos saugumo politiką, duomenų tvarkymo teisėtumą, valstybės informacinių sistemų tvarkytojų veiklą ir duomenų saugos valdymą.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

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

14. 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.

15. Pagrindinės nuostatos dėl rizikos veiksnių vertinimo:

15.1. ŽŪKVR rizikos vertinimą inicijuoja ŽŪKVR valdytojas;

15.2. ŽŪKVR informacinės saugos rizika nustatoma periodinio rizikos vertinimo metu;

15.3. ŽŪKVR rizikos vertinimas atliekamas ne rečiau kaip kartą per metus. Vertinimo

metu:

15.3.1. įvertinama saugos nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų atitiktis esamai ŽŪKVR duomenų saugos situacijai;

15.3.2. inventorizuojama ŽŪKVR techninė ir programinė įranga;

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

15.4. ŽŪKVR rizikos veiksniai vertinami taikant kokybinę rizikos vertinimo metodiką;

15.5. ŽŪKVR vertinimas atliekamas vadovaujantis:

15.5.1. Lietuvos Respublikos duomenų saugą reglamentuojančiais teisės aktų reikalavimais;

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

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

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

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

15.6.3. nenugalima jėga (*force majeure*);

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

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

16.1. įvertinama saugos nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų atitiktis realiai ŽŪKVR duomenų saugos situacijai;

16.2. inventorizuojama ŽŪKVR techninė ir programinė įranga;

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

16.4. patikrinama ŽŪKVR naudotojams suteiktų teisių ir vykdomų funkcijų atitiktis;

16.5. įvertinamas pasirengimas užtikrinti ŽŪKVR veiklos tęstinumą įvykus saugos incidentui;

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

17. ŽŪKVR saugos priemonės parenkamos įvertinus galimus ŽŪKVR duomenų vientisumo, konfidencialumo ir prieinamumo rizikos veiksnius.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

18. Metodai ir priemonės, kurie taikomi užtikrinant prieigą prie ŽŪKVR:

18.1. prieigos prie ŽŪKVR teises suteikia ŽŪKVR administratorius. Pasikeitus ŽŪKVR naudotojo pareigoms ar atliekamoms užduotims, suteikta prieiga prie ŽŪKVR turi būti nedelsiant užblokuojama. ŽŪKVR naudotojams suteiktos prieigos teisės periodiškai, bet ne rečiau kaip kartą per metus, turi būti peržiūrimos, siekiant nustatyti ir pašalinti subjektus,

kuriems prieigos teisės prie ŽŪKVR turi būti panaikintos arba pakeistos. Už periodinę ŽŪKVR naudotojų teisių peržiūrą atsakingas ŽŪKVR saugos įgaliotinis;

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

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

18.4. ŽŪKVR naudotojų prieigai prie ŽŪKVR naudojamas šifruotas HTTPS duomenų perdavimo protokolas bei interneto naršyklė.

19. ŽŪKVR 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 ŽŪKVR nuo kenksmingos programinės įrangos, naudojimo nuostatos:

19.1. ŽŪKVR funkcionuoti būtina programinė tarnybinių stočių ir ŽŪKVR 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 ŽŪKVR administratorius;

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

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

19.4. ŽŪKVR naudotojų kompiuteriai turi būti apsaugoti lokaliomis ugniasienėmis;

19.5. ŽŪKVR 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.

20. Programinės įrangos naudojimo ribojimo nuostatos:

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

21. Kompiuterių tinklo filtravimo įrangos naudojimo nuostatos:

21.1. ŽŪKVR elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų telekomunikacijos tinklų naudojant užkardą;

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

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

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

22. Leistinos kompiuterių (įskaitant nešiojamuosius) naudojimo ribos:

22.1. stacionarieji ir nešiojamieji ŽŪKVR 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 ŽŪKVR elektroninė informacija;

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

23. Metodai, kurie leidžiami užtikrinant saugų ŽŪKVR elektroninės informacijos

teikimą ir (ar) gavimą:

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

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

24. Pagrindiniai atsarginių ŽŪKVR duomenų kopijų darymo ir atkūrimo reikalavimai:

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

24.2. atsarginės ŽŪKVR duomenų kopijos turi būti daromos ir jų atkūrimas turi būti atliekamas pagal VĮ Žemės ūkio informacijos ir kaimo verslo centro svarbiausios veiklos atsarginių kopijų administravimo procedūros aprašą, patvirtintą VĮ Žemės ūkio informacijos ir kaimo verslo centro generalinio direktoriaus;

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

IV. REIKALAVIMAI PERSONALUI

25. ŽŪKVR 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 ŽŪKVR saugos politika.

26. ŽŪKVR administratorius privalo išmanyti ŽŪKVR 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.

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

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

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

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

31. Už ŽŪKVR naudotojų supažindinimą su ŽŪKVR 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 ŽŪKVR saugos įgaliotinis.

V. BAIGIAMOSIOS NUOSTATOS

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

_____