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

DĖL LIETUVOS RESPUBLIKOS TRAKTORIŲ, SAVAEIGIŲ IR ŽEMĖS ŪKIO MAŠINŲ IR JŲ PRIEKABŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO IR ŽEMĖS ŪKIO MINISTRO 2007 M. VASARIO 1 D. ĮSAKYMO NR. 3D-40 PRIPAŽINIMO NETEKUSIU GALIOS

2013 m. sausio 16 d. Nr. 3D-49
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), 6 punktu:

1. T v i r t i n u Lietuvos Respublikos traktorių, savaeigių ir žemės ūkio mašinų ir jų priekabų 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 suderinus su Lietuvos Respublikos vidaus reikalų ministerija teikti tvirtinti.

2.2. Valstybės įmonei Žemės ūkio informacijos ir kaimo verslo centrui per 14 darbo dienų nuo šio įsakymo įsigaliojimo datos paskirti Lietuvos Respublikos traktorių, savaeigių ir žemės ūkio mašinų ir jų priekabų registro duomenų saugos įgaliotinį.

3. P r i p a ž į s t u netekusiu galios Lietuvos Respublikos žemės ūkio ministro 2007 m. vasario 1 d. įsakymą Nr. 3D-40 „Dėl Traktorių, savaeigių ir žemės ūkio mašinų ir jų priekabų registro duomenų saugos nuostatų patvirtinimo“ (Žin., 2007, Nr. 18-682).

ŽEMĖS ŪKIO MINISTRAS VIGILIJUS JUKNA

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2013 m. sausio 9 d. raštu Nr. 1D-294(52)

PATVIRTINTA
Lietuvos Respublikos žemės ūkio ministro
2013 m. sausio 16 d. įsakymu Nr. 3D-49

LIETUVOS RESPUBLIKOS TRAKTORIŲ, SAVAEIGIŲ IR ŽEMĖS ŪKIO MAŠINŲ IR JŲ PRIEKABŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos traktorių, savaeigių ir žemės ūkio mašinų ir jų priekabų registro (toliau – TSMPR) duomenų saugos nuostatai (toliau – saugos nuostatai) nustato TSMPR saugos politiką. Saugos politikos įgyvendinimo tvarką nustato TSMPR saugaus elektroninės informacijos tvarkymo taisyklės, TSMPR veiklos tęstinumo valdymo planas, TSMPR naudotojų administravimo taisyklės, kurias tvirtina TSMPR valdytojas.

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

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

5. Elektroninės TSMPR duomenų saugos užtikrinimo prioritetinės kryptys:

5.1. TSMPR duomenų konfidencialumo užtikrinimas;

5.2. TSMPR reikalaujamo prieinamumo lygio užtikrinimas;

5.3. prieigos prie TSMPR kontrolė;

5.4. TSMPR naudotojų mokymas.

6. Saugos nuostatai taikomi:

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

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

6.3. TSMPR naudotojams;

6.4. TSMPR administratoriui;

6.5. TSMPR saugos įgaliotiniui.

7. TSMPR valdytojo funkcijos ir atsakomybė:

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

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

7.3. vadovauja TSMPR tvarkytojo veiklai kuriant ir diegiant TSMPR, taip pat užtikrina TSMPR veikimą, tobulinimą;

7.4. priima sprendimus dėl TSMPR rizikos veiksnių vertinimo atlikimo;

7.5. atlieka kitas saugos nuostatų, TSMPR nuostatų ir kitų teisės aktų nustatytas funkcijas;

7.6. pagal kompetenciją atsako už registro duomenų ir registro informacijos saugą;

7.7. paveda TSMPR tvarkytojui skirti TSMPR saugos įgaliotinį.

8. TSMPR tvarkytojo funkcijos ir atsakomybė:

8.1. užtikrina TSMPR prieinamumą;

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

8.5. TSMPR valdytojo raštišku pavedimu skiria TSMPR saugos įgaliotinį;

8.6. TSMPR valdytojo raštišku pavedimu skiria TSMPR administratorių;

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

9. TSMPR saugos įgaliotinio funkcijos ir atsakomybė:

9.1. teikia TSMPR tvarkytojo vadovui pasiūlymus dėl:

9.1.1. TSMPR administratoriaus paskyrimo;

9.1.2. TSMPR saugos dokumentų priėmimo, keitimo arba panaikinimo;

9.1.3. TSMPR tvarkytojo informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

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

9.3. teikia TSMPR administratoriui privalomus vykdyti nurodymus ir pavedimus;

9.4. TSMPR tvarkytojo nustatyta tvarka, supažindina TSMPR tvarkytojo darbuotojus, TSMPR administratorių ir TSMPR naudotojus su saugos nuostatais, saugos politiką įgyvendinančių 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 TSMPR elektroninės informacijos saugos įgyvendinimą;

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

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

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

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

10. TSMPR administratoriaus funkcijos ir atsakomybė:

10.1. užtikrina TSMPR serverių srities funkcionavimą ir prieigų prie TSMPR teisių suteikimą;

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

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

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

10.5. atlieka TSMPR priežiūrą.

11. TSMPR naudotojų funkcijos:

11.1. rūpintis TSMPR ir joje tvarkomos informacijos saugumu;

11.2. tvarkyti ir naudoti TSMPR duomenis, vykdant tiesiogines su darbu susijusias funkcijas;

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

12. Teisės aktai, kuriais vadovaujamasi tvarkant TSMPR, 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. 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);

12.8. 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);

12.9. 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);

12.10. 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. TSMPR 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 TSMPR tvarkomų asmens duomenų TSMPR yra priskiriamas 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 TSMPR saugomus asmens duomenis TSMPR priskiriamas antrasis saugumo lygis.

14. Pagrindinės nuostatos dėl rizikos veiksnių vertinimo:

14.1. TSMPR rizikos vertinimą inicijuoja TSMPR valdytojas.

14.2. TSMPR informacinės saugos rizika nustatoma periodinio rizikos vertinimo metu.

14.3. TSMPR rizikos vertinimas atliekamas ne rečiau kaip kartą per metus;

14.4. AVIS saugos įgaliotinis yra atsakingas už AVIS rizikos vertinimo atlikimo organizavimą;

14.5. TSMPR rizikos veiksniai vertinami taikant kokybinę rizikos vertinimo metodiką.

14.6. TSMPR vertinimas atliekamas vadovaujantis:

14.6.1. Lietuvos Respublikos duomenų saugą reglamentuojančiais teisės aktų reikalavimais;

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

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

14.7.1. 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);

14.7.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis TSMPR 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. TSMPR valdytojas, atsižvelgdamas į TSMPR rizikos įvertinimo ataskaitą, prireikus tvirtina TSMPR 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, TSMPR saugos įgaliotinis ne rečiau kaip kartą per 2 metus organizuoja TSMPR informacinių technologijų saugos atitikties vertinimą, kurio metu:

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

15.2. inventorizuojama TSMPR techninė ir programinė įranga;

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

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

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

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

16. TSMPR saugos priemonės parenkamos įvertinus galimus rizikos veiksnius TSMPR duomenų vientisumui, konfidencialumui ir prieinamumui.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

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

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

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

17.3. Kiekvienas TSMPR naudotojas sistemoje turi būti unikaliai atpažįstamas pagal jam suteiktą atpažinties kodą ir atitinkamą slaptažodį.

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

18. TSMPR 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 TSMPR nuo kenksmingos programinės įrangos, naudojimo nuostatos:

18.1. TSMPR funkcionuoti būtina programinė tarnybinių stočių ir TSMPR 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 programinę įrangos kontrolę atsakingas TSMPR saugos įgaliotinis.

18.2. TSMPR funkcionuoti būtina serverių srities ir TSMPR 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 TSMPR saugos įgaliotinis.

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

18.4. TSMPR naudotojų kompiuteriai turi būti apsaugoti lokaliomis ugniasienėmis.

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

20. Kompiuterių tinklo filtravimo įrangos naudojimo nuostatos:

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

20.2. Konfigūruojant TSMPR elektroninės informacijos perdavimo tinklo užkardas, turi būti naudojami tik organizacijos veiklai būtini tinklo protokolai ir užkardų prievadai.

20.3. TSMPR saugos įgaliotinis organizuoja TSMPR serverių srities tinklo užkardų administravimą, priežiūrą, operacinės sistemos atnaujinimą ir saugią užkardų konfigūraciją.

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

21. Leistinos kompiuterių (įskaitant nešiojamus) naudojimo ribos:

21.1. Stacionarūs ir nešiojami TSMPR naudotojų kompiuteriai privalo būti naudojami tik su tiesioginių pareigų atlikimu susijusiai veiklai atlikti. Iš kompiuterių, kurie perduodami remontui ar techniniam aptarnavimui, turi būti pašalinta visa riboto naudojimo TSMPR elektroninė informacija.

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

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

22.1. TSMPR duomenys perduodami automatiniu būdu TCP/IP protokolu realiu laiku arba asinchroniniu režimu pagal TSMPR 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 TSMPR saugos įgaliotinis.

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

23.1. Atsarginių TSMPR duomenų kopijų darymas ir atkūrimas turi būti atliekamas laikantis Lietuvos Respublikos teisės aktų nustatytų reikalavimų.

23.2. Atsarginės TSMPR 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.

23.3. Už atsarginių TSMPR duomenų kopijų darymo ir atkūrimo bei už TSMPR

taikomosios programinės įrangos (aplikacijų) kopijų darymo organizavimą ir peržiūrą yra atsakingas TSMPR saugos įgaliotinis.

IV. REIKALAVIMAI PERSONALUI

24. TSMPR 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 TSMPR saugos politika.

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

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

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

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

29. Visi TSMPR naudotojai privalo būti supažindinti su TSMPR saugos dokumentais, savo pareigomis ir atsakomybe, susijusia su TSMPR elektroninės informacijos sauga bei teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą bei raštu sutikę laikytis jų reikalavimų.

30. AVIS naudotojų elektroninės informacijos saugos mokymai ir žinių atnaujinimas atliekamas kasmet. Elektroninės informacijos saugos mokymus organizuoja saugos įgaliotinis.

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

V. BAIGIAMOSIOS NUOSTATOS

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

_____