LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO MINISTRAS

ĮSAKYMAS
DĖL TRAKTORININKO PAŽYMĖJIMŲ INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2017 m. lapkričio 2 d. Nr. 3D-699

Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 8 straipsnio 3 dalimi ir 30 straipsniu, 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“, 9 punktu, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ 7, 11 ir 19 punktais, atsižvelgdamas į Traktorių ir savaeigių mašinų vairuotojų (traktorininkų) mokymo ir teisės vairuoti šias transporto priemones įgijimo tvarkos aprašą ir Traktorių ir savaeigių mašinų vairuotojų (traktorininkų) pažymėjimų išdavimo ir keitimo tvarkos aprašą, patvirtintus Lietuvos Respublikos žemės ūkio ministro 2009 m. liepos 10 d. įsakymu Nr. 3D-498 „Dėl Traktorių ir savaeigių mašinų vairuotojų (traktorininkų) mokymo ir teisės vairuoti šias transporto priemones įgijimo tvarkos aprašo bei traktorių ir savaeigių mašinų vairuotojų (traktorininkų) pažymėjimų išdavimo tvarkos aprašo patvirtinimo“, ir Lietuvos Respu

1. T v i r t i n u Traktorininko pažymėjimų informacinės sistemos duomenų saugos nuostatus (pridedama).

2 . P a v e d u :

2.1. Žemės ūkio ministerijos Veiklos administravimo ir turto valdymo departamento Informacinių sistemų skyriui ne vėliau kaip per 5 darbo dienas nuo šio įsakymo įsigaliojimo dienos pateikti šio įsakymo ir juo tvirtinamų dokumentų kopijas Registrų ir valstybės informacinių sistemų registrui Registrų ir valstybės informacinių sistemų registro nuostatų numatyta tvarka;

2.2. VĮ Žemės ūkio informacijos ir kaimo verslo centrui paskirti Traktorininko pažymėjimų informacinės sistemos saugos įgaliotinį ir administratorių;

2.3. saugos įgaliotiniui pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų numatyta tvarka rizikos įvertinimo rezultatus;

3. šio įsakymo vykdymą kontroliuoti žemės ūkio viceministrui pagal administravimo sritį.

Žemės ūkio ministras Bronius Markauskas

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2017-10-16 raštu Nr. 1D-5438

PATVIRTINTA
Lietuvos Respublikos žemės ūkio ministro
2017 m. lapkričio 2 d. įsakymu Nr. 3D-699

TRAKTORININKO PAŽYMĖJIMŲ INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Traktorininko pažymėjimų informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Traktorininko pažymėjimų informacinės sistemos elektroninės informacijos saugos politiką.

2. Saugos nuostatuose vartojamos sąvokos:

2.1. **Traktorininko pažymėjimų informacinė sistema** (toliau – TPIS) – duomenų apie Lietuvoje išduodamus ir keičiamus traktorininko pažymėjimus kaupimo ir informacijos apie juos teikimo sistema.

2.2. **TPIS administratorius** – TPIS tvarkytojo paskirtas darbuotojas, prižiūrintis TPIS ir (ar) jos infrastruktūrą, užtikrinantis jos veikimą ir elektroninės informacijos saugą.

2.3. **TPIS naudotojas** – valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, turintis teisę naudotis TPIS ištekliais numatytoms funkcijoms atlikti.

2.4. **TPIS naudotojų administratorius** – TPIS tvarkytojo paskirtas darbuotojas, administruojantis TPIS naudotojų prieigos teisių valdymą ir atliekantis kitas teisės aktų nustatytas funkcijas.

2.5. **TPIS saugos įgaliotinis** – TPIS tvarkytojo paskirtas darbuotojas, koordinuojantis ir prižiūrintis elektroninės informacijos saugos politikos įgyvendinimą TPIS.

2.6. Kitos Saugos nuostatuose vartojamos sąvokos apibrėžtos Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Saugos dokumentų turinio gairių ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių apraše, patvirtintuose Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, kituose teisės aktuose.

3. TPIS tvarkomos elektroninės informacijos saugos užtikrinimo tikslas – sudaryti sąlygas saugiai automatizuotu būdu tvarkyti ir saugoti elektroninę informaciją TPIS, užtikrinti elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą.

4. TPIS informacijos saugumui užtikrinti naudojamos organizacinės, techninės, programinės ir fizinės informacijos apsaugos priemonės.

5. TPIS elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

5.1. TPIS elektroninės informacijos konfidencialumo užtikrinimas;

5.2. TPIS elektroninės informacijos vientisumo užtikrinimas;

5.3. TPIS elektroninės informacijos prieinamumo užtikrinimas;

5.4. prieigos prie TPIS kontrolė;

5.5. TPIS rizikos valdymas;

5.6. TPIS veiklos tęstinumo užtikrinimas;

5.7. TPIS naudotojų ir TPIS administratoriaus saugos mokymas.

6. Saugos nuostatai taikomi:

6.1. TPIS valdytojai – Lietuvos Respublikos žemės ūkio ministerijai (toliau – TPIS valdytojas), Gedimino pr. 19, 01103 Vilnius;

6.2. TPIS tvarkytojui – VĮ Žemės ūkio informacijos ir kaimo verslo centrui (toliau – ŽŪIKVC), V. Kudirkos g. 18-1, 03105 Vilnius;

6.3. TPIS naudotojams;

6.4. TPIS administratoriui;

6.5. TPIS naudotojų administratoriui;

6.6. TPIS saugos įgaliotiniui.

7. TPIS valdytojo funkcijos:

7.1. rengti ir priimti teisės aktus, užtikrinančius TPIS duomenų tvarkymo teisėtumą ir TPIS elektroninės informacijos saugą, atlikti teisės aktų nuostatų laikymosi priežiūrą;

7.2. nagrinėti TPIS tvarkytojo pasiūlymus dėl TPIS veiklos, elektroninės informacijos saugos, juos apibendrinti ir priimti sprendimus dėl TPIS tobulinimo;

7.3. metodiškai vadovauti TPIS tvarkytojo veiklai kuriant ir diegiant TPIS, taip pat užtikrinant TPIS veikimą, tobulinimą ir elektroninės informacijos saugą;

7.4. rengti TPIS biudžeto projektus;

7.5. pavesti TPIS tvarkytojui skirti TPIS saugos įgaliotinį ir TPIS administratorių;

7.6. priimti sprendimus dėl TPIS rizikos vertinimo rezultatų;

7.7. atlikti kitas Saugos nuostatuose, TPIS nuostatuose ir kituose teisės aktuose pavestas funkcijas.

8. TPIS tvarkytojo funkcijos:

8.1. užtikrinti TPIS prieinamumą;

8.2. užtikrinti TPIS duomenų atsarginių kopijų darymą;

8.3. pagal kompetenciją užtikrinti TPIS veiklos tęstinumą;

8.4. užtikrinti TPIS taikomajai programinei įrangai, tarnybinėms stotims ir juose esantiems duomenims funkcionuoti būtinos informacinių technologijų infrastruktūros (toliau – serverių sritis) saugą;

8.5. priimti sprendimus dėl TPIS rizikos vertinimo rezultatų;

8.6. rengti ir saugoti serverių srities saugai užtikrinti būtiną dokumentaciją;

8.7. sudaryti TPIS duomenų gavimo ir teikimo sutartis ir užtikrinti duomenų gavimo ir teikimo saugą;

8.8. sudaryti galimybes duomenų teikėjams teikti duomenis elektroniniu būdu;

8.9. užtikrinti TPIS elektroninės informacijos saugą;

8.10. skirti TPIS saugos įgaliotinį;

8.11. skirti TPIS administratorių;

8.12. skirti TPIS naudotojų administratorių;

8.13. teikti pastabas ir pasiūlymus TPIS valdytojui TPIS veiklos klausimais;

8.14. atlikti kitas Saugos nuostatuose, TPIS nuostatuose ir kituose teisės aktuose pavestas funkcijas.

9. TPIS saugos įgaliotinio funkcijos:

9.1. teikti TPIS tvarkytojo vadovui pasiūlymus dėl:

9.1.1. TPIS administratoriaus paskyrimo ir elektroninės informacijos saugos reikalavimų nustatymo;

9.1.2. saugos dokumentų priėmimo, keitimo ir panaikinimo;

9.1.3. TPIS tvarkytojo informacinių technologijų saugos atitikties vertinimo atlikimo;

9.2. koordinuoti įvykusių incidentų dėl TPIS elektroninės informacijos saugos tyrimą;

9.3. teikti TPIS administratoriui privalomus vykdyti nurodymus ir pavedimus, susijusius su Informacijos saugumo politikos įgyvendinimu;

9.4. organizuoti TPIS naudotojų supažindinimą su TPIS saugos dokumentais, užtikrinti supažindinimo įrodomumą;

9.5. koordinuoti TPIS saugos dokumentų reikalavimų vykdymą;

9.6. organizuoti ir atlikti TPIS rizikos vertinimą;

9.7. atlikti kitas Saugos nuostatuose ir kituose saugos dokumentuose pavestas funkcijas.

10. TPIS administratoriaus funkcijos:

10.1. atsakyti už TPIS tarnybinių stočių funkcionavimą ir prieigų prie TPIS infrastruktūros išteklių teisių suteikimą;

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

10.3. nustatyti TPIS pažeidžiamas vietas;

10.4. reaguoti į elektroninės informacijos saugos incidentus;

10.5. patikrinti (peržiūrėti) TPIS sąranką ir TPIS būsenos rodiklius reguliariai, ne rečiau kaip kartą per metus ir (arba) po TPIS pokyčio;

10.6. įgyvendinti TPIS pokyčius, kuriuos inicijuoja TPIS duomenų valdymo įgaliotinis, saugos įgaliotinis arba pats administratorius;

10.7. pagal kompetenciją teikti pasiūlymus TPIS saugos įgaliotiniui dėl TPIS palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir TPIS elektroninės informacijos saugos užtikrinimo;

10.8. informuoti TPIS saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikti pasiūlymus dėl jų pašalinimo;

10.9. vykdyti visus TPIS saugos įgaliotinio nurodymus ir pavedimus, susijusius su TPIS elektroninės informacijos saugos užtikrinimu;

10.10. teikti TPIS saugos įgaliotiniui informaciją apie TPIS elektroninės informacijos saugą užtikrinančių komponentų būklę;

10.11. atlikti kitas Saugos nuostatuose ir kituose saugos dokumentuose pavestas funkcijas.

11. TPIS naudotojų administratoriaus funkcijos:

11.1. vykdyti prieigų prie TPIS suteikimą;

11.2. vykdyti TPIS teisių valdymą;

11.3. redaguoti TPIS naudotojų teises;

11.4. atlikti kitas Saugos nuostatuose ir kituose saugos dokumentuose pavestas funkcijas.

12. TPIS naudotojo funkcijos:

12.1. atsakyti už TPIS ir joje tvarkomų duomenų saugumą;

12.2. tvarkyti TPIS elektroninę informaciją;

12.3. neatskleisti, neperduoti tvarkomos TPIS elektroninės informacijos;

12.4. atlikti kitas Saugos nuostatų, TPIS nuostatų ir kitų teisės aktų nustatytas funkcijas.

13. Teisės aktai, kuriais vadovaujamasi tvarkant elektroninę informaciją ir užtikrinant jos saugą:

13.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

13.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

13.3. Lietuvos Respublikos kibernetinio saugumo įstatymas;

13.4. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, saugos dokumentų turinio gairių aprašas ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės svarbos nustatymo gairių aprašas;

13.5. Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“;

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

13.7. Organizaciniai ir techniniai kibernetinio saugumo reikalavimai, taikomi ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, patvirtinti Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“;

13.8. 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) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms asmens duomenų saugumo priemonėms patvirtinimo“;

13.9. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

13.10. Lietuvos standartai LST ISO/IEC 27002:2014 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ ir LST ISO/IEC 27001:2013 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“ ir kiti Lietuvos ir tarptautiniai standartai, reglamentuojantys informacijos saugumą;

13.11. kiti teisės aktai, reglamentuojantys elektroninės informacijos saugą valstybės institucijose.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

14. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašu, TPIS tvarkoma elektroninė informacija priskiriama vidutinės svarbos elektroninės informacijos kategorijai, kadangi dėl šios elektroninės informacijos konfidencialumo, vientisumo ir (ar) prieinamumo praradimo gali kilti grėsmė, kad prasidės Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo 9.1–9.6 papunkčiuose nurodyti procesai.

15. Pagal TPIS tvarkomą vidutinės svarbos elektroninę informaciją TPIS priskiriama prie trečiosios kategorijos informacinių sistemų.

16. Vadovaujantis Bendraisiais reikalavimais organizacinėms ir techninėms asmens duomenų saugumo priemonėms dėl galimybės per išorinius duomenų perdavimo tinklus tvarkyti TPIS saugomus asmens duomenis TPIS priskiriamas prie antrojo saugumo lygio.

17. TPIS saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, kuri skelbiama Vidaus reikalų ministerijos interneto svetainėje (adresu http://www.vrm.lt/Rizikos_analize.pdf) (toliau – Vidaus reikalų ministerijos išleista metodinė priemonė „Rizikos analizės vadovas“), Lietuvos ir tarptautinius standartus „Informacijos technologija. Saugumo technika“, kasmet organizuoja TPIS rizikos vertinimą. Prireikus TPIS saugos įgaliotinis gali organizuoti neeilinį TPIS rizikos vertinimą. TPIS tvarkytojo rašytiniu pavedimu TPIS rizikos vertinimą gali atlikti pats TPIS saugos įgaliotinis. TPIS

rizikos vertinimo rezultatai išdėstomi Rizikos įvertinimo ataskaitoje, kuri pateikiama TPIS tvarkytojo vadovui. Rizikos įvertinimo ataskaita rengiama vertinant rizikos veiksnius, galinčius turėti įtakos TPIS elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausi rizikos veiksniai:

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

17.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis TPIS elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymas, saugos pažeidimai, vagystės ir kita);

17.3. 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.

18. Pagrindinės nuostatos dėl rizikos veiksnių vertinimo:

18.1. TPIS rizikos vertinimą inicijuoja TPIS valdytojas ar TPIS tvarkytojas;

18.2. TPIS rizika nustatoma periodinio rizikos vertinimo metu;

18.3. TPIS rizikos vertinimas atliekamas ne rečiau kaip kartą per metus;

18.4. TPIS saugos įgaliotinis yra atsakingas už TPIS rizikos vertinimo atlikimo organizavimą;

18.5. TPIS rizikos veiksniai vertinami taikant TPIS tvarkytojo patvirtintą Rizikos vertinimo metodiką.

19. TPIS rizikos vertinimas atliekamas vadovaujantis:

19.1. Lietuvos Respublikos valstybės institucijų ir įstaigų informacinių sistemų duomenų saugą reglamentuojančių teisės aktų reikalavimais;

19.2. Lietuvos standartu LST ISO/IEC 27001:2013 ir kitais Lietuvos ir tarptautiniais standartais, reglamentuojančiais rizikos vertinimą;

19.3. TPIS tvarkytojo patvirtinta Informacijos saugumo politika;

19.4. TPIS tvarkytojo patvirtintu Rizikos valdymo tvarkos aprašu.

20. Rizikos valdymo procesą sudaro rizikos vertinimo konteksto nustatymas, rizikos vertinimas (informacinių išteklių inventorizacija ir jų įtakos TPIS tvarkytojo veiklai vertinimas, rizikos analizė, rizikos įvertinimas), rizikos tvarkymas ir rizikos stebėsena ir peržiūra.

21. TPIS valdytojas, atsižvelgdamas į TPIS rizikos vertinimo rezultatus, prireikus tvirtina TPIS saugos įgaliotinio parengtą Rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

22. TPIS saugos užtikrinimo priemonės parenkamos vadovaujantis:

22.1. Lietuvos Respublikos kibernetinio saugumo įstatymu;

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

22.3. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašu;

22.4. Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašu, nustatančiu būtinas priemones pagal informacinei sistemai priskirtą saugos kategoriją;

22.5. Bendraisiais reikalavimais organizacinėms ir techninėms asmens duomenų saugumo priemonėms;

22.6. Vidaus reikalų ministerijos išleista metodine priemone „Rizikos analizės vadovas“;

22.7. kitų elektroninės informacijos saugą reglamentuojančių Lietuvos Respublikos teisės aktų, nustatančių būtinas priemones pagal informacinei sistemai priskirtą kategoriją, reikalavimais;

22.8. Lietuvos standarte LST ISO/IEC 27001:2013 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai rekomendacijomis ir siūlymais.

23. Pagrindiniai elektroninės informacijos saugos priemonių parinkimo principai yra šie:

23.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

23.2. elektroninės informacijos saugos priemonės diegimo kaina turi būti proporcinga saugomos elektroninės informacijos vertei;

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

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

24. Programinės įrangos, skirtos apsaugoti TPIS nuo kenksmingos programinės įrangos, naudojimo nuostatos:

24.1. TPIS funkcionuoti būtina programinė tarnybinių stočių ir TPIS 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 konfigūravimą atsakingas TPIS administratorius, o už kontrolę – TPIS saugos įgaliotinis.

24.2. TPIS funkcionuoti būtina tarnybinėse stotyse ir TPIS naudotojų kompiuteriuose esanti programinė įranga turi būti atnaujinama ne vėliau kaip per 5 darbo dienas po programinės įrangos gamintojų pranešimo apie programinės įrangos atnaujinimą. Už serverių srities atnaujinimo atlikimą atsakingas TPIS administratorius, o už kontrolę – TPIS saugos įgaliotinis.

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

24.4. TPIS naudotojų kompiuteriai turi būti apsaugoti lokaliomis saugasienėmis.

24.5. TPIS 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.

25. Programinės įrangos naudojimo ribojimo nuostatos:

25.1. TPIS tarnybinėse stotyse turi veikti tik legali programinė įranga;

25.2. periodiškai, bet ne rečiau kaip kartą per metus, turi būti atliekamas TPIS rizikos vertinimas ir informacinių technologijų saugos atitikties vertinimas, kuriuos inicijuoja TPIS saugos įgaliotinis.

26. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotojų serverių ir kitos) naudojimo nuostatos:

26.1. TPIS naudotojų elektroninės informacijos perdavimo tinklo ir užkardų priežiūra vykdoma pagal TPIS tvarkytojo patvirtintą Kompiuterinio tinklo konfigūravimo ir stebėsenos tvarkos aprašą;

26.2. tinklo ir užkardų konfigūracija peržiūrima ne rečiau kaip kartą per metus. Peržiūrą inicijuoja TPIS saugos įgaliotinis, o ją vykdo TPIS administratorius;

26.3. visas duomenų srautas į internetą ir iš jo filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos;

26.4. naudojamos turinio filtravimo sistemos;

26.5. naudojamos taikomųjų programų kontrolės sistemos;

26.6. apsaugai nuo elektroninės informacijos nutekinimo turi būti naudojama duomenų srautų analizės ir kontrolės įranga, galinti iššifruoti įeinančių ir išeinančių duomenų srautų duomenis.

27. Leistinos TPIS naudotojų kompiuterių naudojimo ribos:

27.1. stacionarūs ir nešiojamieji TPIS 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 TPIS apriboto naudojimo elektroninė informacija;

27.2. visiems TPIS naudotojų kompiuteriams privaloma naudoti papildomas saugos priemones, kuriomis patvirtinama kompiuterio TPIS naudotojo tapatybė ir šifruojami duomenys.

28. Metodai, kuriais galima užtikrinti saugų TPIS elektroninės informacijos teikimą ir (ar) gavimą:

28.1. TPIS duomenys perduodami automatiškai TCP/IP protokolu realiuoju laiku arba asinchroniniu režimu pagal TPIS duomenų teikimo ir gavimo sutartis, kuriose nustatytos perduodamų duomenų specifikacijos, perdavimo sąlygos ir tvarka;

28.2. už duomenų teikimo ir gavimo sutartyse nurodomų saugos reikalavimų nustatymą, suformulavimą ir įgyvendinimo organizavimą atsakingas TPIS saugos įgaliotinis;

28.3. TPIS duomenų perdavimas šifruotais ryšio kanalais;

28.4. duomenų registravimui naudojamas saugus HTTPS protokolas;

28.5. saugaus valstybinio duomenų perdavimo tinklo (SVDPT) naudojimas.

29. Pagrindiniai atsarginių TPIS duomenų kopijų darymo ir atkūrimo reikalavimai:

29.1. atsarginių TPIS duomenų kopijų darymas ir atkūrimas turi būti atliekamas laikantis Lietuvos Respublikos teisės aktų reikalavimų;

29.2. atsarginės TPIS duomenų kopijos turi būti daromos periodiškai (visų duomenų kopija – vieną kartą per savaitę) pagal TPIS tvarkytojo patvirtintą Svarbiausių veiklos duomenų ir kitos informacijos atsarginių kopijų administravimo tvarkos aprašą;

29.3. atsarginių kopijų laikmenos yra pažymimos taip, kad jas būtų galima atpažinti;

29.4. TPIS duomenų atkūrimas iš atsarginių duomenų kopijų turi būti periodiškai išbandomas pagal ŽŪIKVC patvirtintą Svarbiausių veiklos duomenų ir kitos informacijos atsarginių

kopijų administravimo tvarkos aprašą. Bandymų eiga ir rezultatai pateikiami TPIS saugos įgaliotiniui;

29.5. už atsarginių TPIS duomenų kopijų darymą ir atkūrimą, už TPIS taikomosios programinės įrangos (aplikacijų) kopijų inicijavimą atsakingas TPIS saugos įgaliotinis, o už vykdymą – TPIS administratorius;

29.6. atsarginės TPIS duomenų kopijos turi būti saugomos užrakintoje nedegioje spintoje, kitose patalpose arba kitame pastate, nei yra įrašymo įrenginys.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

30. TPIS saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų duomenų tvarkymą, standartais ir kitais dokumentais, sugebėti prižiūrėti, kaip įgyvendinama TPIS elektroninės informacijos saugumo politika, tobulinti kvalifikaciją elektroninės informacijos saugos srityje.

31. TPIS 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.

32. TPIS administratorius privalo išmanyti TPIS elektroninės informacijos saugumo politikos principus, mokėti dirbti su duomenų perdavimo tinklais, užtikrinti jų saugą, taip pat administruoti ir prižiūrėti informacines sistemas, turi būti susipažinęs su šiais Saugos nuostatais ir kitais su elektroninės informacijos sauga susijusiais dokumentais, darbo saugos taisyklėmis.

33. TPIS administratorius privalo sugebėti užtikrinti techninės ir programinės įrangos nepertraukiamą funkcionavimą, stebėti techninės ir programinės įrangos veikimą, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, sutrikimų diagnostiką ir šalinimą, išmanyti elektroninės informacijos saugos užtikrinimo principus.

34. TPIS naudotojai privalo išmanyti Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymą ir kitus teisės aktus, reglamentuojančius asmens duomenų saugą, turi turėti

naudojimosi kompiuteriu įgūdžių, būti susipažinę su Saugos nuostatais ir kitais susijusiais saugos dokumentais.

35. TPIS naudotojai, pastebėję Informacijos saugumo politikos pažeidimų, nusikalstamos veikos požymių ar netinkamai veikiančių TPIS elektroninės informacijos saugos užtikrinimo priemonių, nedelsdami privalo apie tai pranešti TPIS tvarkytojui.

36. TPIS administratorius apie Saugos nuostatų 17 punkte nurodytus rizikos veiksnius informuoja TPIS saugos įgaliotinį. Įtaręs neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeidžiančią TPIS elektroninę informaciją (jos konfidencialumą, vientisumą ar prieinamumą), TPIS saugos įgaliotinis apie tai turi pranešti TPIS tvarkytojo vadovui ir kompetentingoms institucijoms.

37. TPIS naudotojų administratorius turi būti gerai susipažinęs su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu ir kitais teisės aktais, reglamentuojančiais asmens duomenų saugą, žinoti visus sutartinius įsipareigojimus ir teisės aktus, susijusius su TPIS naudotojų administravimu.

38. TPIS naudotojų administratorius turi žinoti TPIS vaidmenis ir jų suteikimo principus.

39. TPIS naudotojų informacijos saugos mokymai ir žinių atnaujinimas atliekamas kasmet, laisvai pasirenkama forma. Už tai atsakingas TPIS saugos įgaliotinis.

V SKYRIUS
TPIS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

40. TPIS naudotojų supažindinimą su saugos dokumentais bei teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinat jos saugumą, jo įrodomumą ir atsakomybę už jų reikalavimų nesilaikymą yra atsakingas TPIS saugos įgaliotinis.

41. Saugos dokumentai yra viešai skelbiami ŽŪIKVC interneto svetainėje.

42. ŽŪIKVC patvirtinta Informacijos saugumo politikos santrauka ir Išorinių naudotojų administravimo taisyklės yra viešai skelbiamos ŽŪIKVC interneto svetainėje ir yra privalomos visiems TPIS naudotojams, dirbantiems su TPIS.

43. Pirmą kartą prisijungęs prie TPIS naudotojas privalo susipažinti su Informacijos saugumo politikos santrauka, Išorinių naudotojų administravimo taisyklėmis, TPIS nuostatais, Saugos nuostatais ir kitais saugos dokumentais.

44. Pasikeitus šių saugos nuostatų 42 punkte nurodytiems dokumentams, TPIS naudotojas privalo su jais pakartotinai susipažinti.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

45. Saugos nuostatai privalomi TPIS valdytojo ir TPIS tvarkytojo darbuotojams, TPIS naudotojams, kurie tvarko TPIS elektroninę informaciją.

46. Asmenys, pažeidę Saugos nuostatus, atsako teisės aktų nustatyta tvarka.

47. Saugos nuostatų ir kitos su TPIS elektroninės informacijos sauga susijusios dokumentacijos priežiūrą ar keitimą inicijuoja TPIS tvarkytojas.

_____