SUDERINTA
Lietuvos Respublikos
vidaus reikalų ministerijos
2018 m. balandžio 20 d. raštu Nr. 1D-2096

Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2018 m. balandžio 12 d. raštu Nr. (4.2)6K-203

PATVIRTINTA
Lietuvos Respublikos
vyriausiosios rinkimų komisijos
2018 m. gegužės 8 d.
sprendimu Nr. Sp-47

LIETUVOS RESPUBLIKOS VYRIAUSIOSIOS RINKIMŲ KOMISIJOS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos vyriausiosios rinkimų komisijos informacinės sistemos duomenų saugos nuostatai (toliau – Nuostatai) nustato Vyriausiosios rinkimų komisijos informacinės sistemos (toliau – VRKIS) elektroninės informacijos saugos politiką.

2. Nuostatuose vartojamos sąvokos:

2.1. **VRKIS naudotojas** – VRKIS valdytojo arba tvarkytojo darbuotojas, dirbantis pagal darbo sutartį, tvarkantis VRKIS elektroninę informaciją.

2.2. **VRKIS administratorius** – VRKIS valdytojo darbuotojas, dirbantis pagal darbo sutartį, prižiūrintis VRKIS ir (ar) jos infrastruktūrą, užtikrinantis jos veikimą, elektroninės informacijos saugą, taip pat šias paslaugas teikiantis paslaugos teikėjas.

2.3. **VRKIS saugos įgaliotinis** – VRKIS valdytojo darbuotojas, koordinuojantis ir prižiūrintis elektroninės informacijos saugos politikos įgyvendinimą (kibernetinio saugumo vadovas).

3. Kitos Nuostatuose vartojamos sąvokos atitinka sąvokas, apibrėžtas Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame 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“, Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 14 d. įsakymu Nr. IV-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), ir kituose teisės aktuose bei Lietuvos „Informacijos technologija. Saugumo metodai“ grupės standartuose.

4. VRKIS elektroninės informacijos saugos tikslas – užtikrinti VRKIS elektroninės informacijos prieinamumą, vientisumą ir konfidencialumą.

5. VRKIS elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

5.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų VRKIS elektroninės informacijos saugai užtikrinti, įgyvendinimas ir šių priemonių įgyvendinimo kontrolė;

5.2. elektroninės informacijos saugos priemonių parinkimas projektavimo ir diegimo metu;

5.3. VRKIS tvarkomų asmens duomenų apsauga;

5.4. VRKIS veiklos tęstinumo užtikrinimas.

6. Nuostatai taikomi:

6.1. VRKIS valdytojui – Lietuvos Respublikos vyriausiajai rinkimų komisijai, Gynėjų g. 8, LT-01109, Vilnius;

6.2. VRKIS pagrindiniam tvarkytojui – Lietuvos Respublikos vyriausiajai rinkimų komisijai, Gynėjų g. 8, LT-01109, Vilnius;

6.3. VRKIS tvarkytojui – Valstybės įmonei Registrų centrui, Vinco Kudirkos g. 18-3, LT-03105, Vilnius;

6.4. VRKIS naudotojams, VRKIS administratoriams, VRKIS saugos įgaliotiniui, VRKIS paslaugų teikėjams.

7. VRKIS valdytojo funkcijos ir atsakomybė:

7.1. organizuoja VRKIS veiklą ir jai vadovauja;

7.2. tvirtina Nuostatus ir VRKIS saugos politiką įgyvendinančius dokumentus;

7.3. priima sprendimą dėl VRKIS informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

7.4. skiria VRKIS saugos įgaliotinį ir paveda jam organizuoti ir kontroliuoti VRKIS saugos politikos įgyvendinimą;

7.5. nustato VRKIS administratoriams keliamus reikalavimus;

7.6. atsako už elektroninės informacijos tvarkymo VRKIS teisėtumą ir saugą.

8. VRKIS pagrindinio tvarkytojo funkcijos ir atsakomybė:

8.1. skiria VRKIS administratorius ir paveda jiems užtikrinti tinkamą VRKIS infrastruktūros veikimą;

8.2. užtikrina nepertraukiamą VRKIS veikimą;

8.3. užtikrina tinkamą elektroninės informacijos saugos teisės aktų ir rekomendacijų

įgyvendinimą;

8.4. kiekvienais metais organizuoja informacijos saugos mokymus VRKIS naudotojams;

8.5. priima sprendimus dėl VRKIS techninių ir programinių priemonių, būtinų VRKIS elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

8.6. nagrinėja pasiūlymus dėl VRKIS saugos tobulinimo ir priima dėl jų sprendimus;

8.7. atlieka kitus teisės aktuose nustatytas funkcijas.

9. VRKIS tvarkytojo funkcijos ir atsakomybė:

9.1. teikia pasiūlymus VRKIS valdytojui dėl VRKIS saugos tobulinimo;

9.2. atsako už elektroninės informacijos saugą savo tvarkymo srityje;

9.3. atlieka kitas teisės aktuose nustatytas funkcijas ir VRKIS valdytojo pavedimus.

10. VRKIS saugos įgaliotinio funkcijos, atsakomybės ir įgaliojimai:

10.1. teikia VRKIS valdytojo vadovui siūlymus dėl:

10.1.1. VRKIS administratorių paskyrimo ir reikalavimų administratoriams nustatymo;

10.1.2. VRKIS informacinių technologijų saugos atitikties vertinimo atlikimo;

10.1.3. VRKIS saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

10.2. koordinuoja ir prižiūri VRKIS saugos politikos įgyvendinimą;

10.3. organizuoja VRKIS informacinių technologijų saugos atitikties vertinimus ir rengia VRKIS informacinių technologijų saugos atitikties vertinimo ataskaitas;

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

10.5. teikia VRKIS administratoriams ir VRKIS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;

10.6. atlikdamas savo funkcijas, turi teisę pagal savo įgaliojimus duoti privalomus vykdyti nurodymus ir pavedimus ir kitiems VRKIS valdytojo ir tvarkytojo darbuotojams, jeigu tai būtina saugos politikai įgyvendinti;

10.7. periodiškai inicijuoja VRKIS naudotojų mokymą informacijos saugos klausimais, įvairiais būdais informuoja juos apie informacijos saugos problematiką;

10.8. kiekvienais metais organizuoja VRKIS rizikos įvertinimą, rengia VRKIS rizikos įvertinimo ataskaitas;

10.9. atlieka kitas Nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas ir kitus VRKIS valdytojo vadovo nurodymus, susijusius su VRKIS elektroninės informacijos sauga.

11. VRKIS administratorių funkcijos ir atsakomybė:

11.1. sisteminių programų ir tarnybinių stočių administratorius:

11.1.1. diegia technines, programines VRKIS saugos priemones ir prižiūri jų veikimą;

11.1.2. pagal kompetenciją techninėmis ir programinėmis priemonėmis užtikrina VRKIS elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą;

11.1.3. techninėmis ir programinėmis priemonėmis registruoja VRKIS elektroninės informacijos saugos incidentus ir informuoja apie juos VRKIS saugos įgaliotinį, teikia VRKIS tvarkytojui pasiūlymus dėl šių incidentų pasekmių pašalinimo;

11.1.4. atlieka įdiegtos VRKIS rezervinio kopijavimo ir atkūrimo sistemos, darančios atsargines VRKIS elektroninės informacijos kopijas bei jas archyvuojančios, priežiūrą, prireikus iš duomenų atsarginių kopijų atkuria VRKIS elektroninę informaciją;

11.1.5. vykdo VRKIS sudedamųjų dalių (operacinių sistemų, duomenų bazių valdymo sistemų, bylų serverių) veikimo koordinavimą, nustato VRKIS pažeidžiamas vietas;

11.1.6. ne rečiau kaip vieną kartą per metus ir (arba) po VRKIS pokyčio patikrina (peržiūri) VRKIS sąranką ir VRKIS būsenos rodiklius;

11.1.7. dalyvauja valdant VRKIS pokyčius, pagal kompetenciją juos įgyvendina;

11.1.8. vykdo VRKIS saugos įgaliotinio nurodymus ir pavedimus, susijusius su VRKIS saugos užtikrinimu;

11.1.9. atlieka kitas VRKIS saugos politiką įgyvendinančiuose dokumentuose nustatytas administratoriaus funkcijas;

11.2. tinklo priežiūros administratorius:

11.2.1. diegia technines, programines VRKIS tinklo saugos priemones ir prižiūri jų veikimą;

11.2.2. pagal kompetenciją techninėmis ir programinėmis priemonėmis užtikrina VRKIS elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą;

11.2.3. techninėmis ir programinėmis priemonėmis registruoja VRKIS elektroninės informacijos saugos incidentus ir informuoja apie juos VRKIS saugos įgaliotinį, teikia VRKIS tvarkytojui pasiūlymus dėl šių incidentų pasekmių pašalinimo;

11.2.4. vykdo VRKIS sudedamųjų dalių (kompiuterių tinklo programinės ir duomenų perdavimo įrangos) veikimo koordinavimą, nustato VRKIS tinklo pažeidžiamas vietas;

11.2.5. dalyvauja valdant VRKIS pokyčius, pagal kompetenciją juos įgyvendina;

11.2.6. vykdo VRKIS saugos įgaliotinio nurodymus ir pavedimus, susijusius su VRKIS saugos užtikrinimu;

11.2.7. atlieka kitas VRKIS saugos politiką įgyvendinančiuose dokumentuose nustatytas administratoriaus funkcijas;

11.3. taikomųjų programų administratorius:

11.3.1. vykdo VRKIS taikomųjų programų sistemų veikimo koordinavimą, nustato VRKIS

pažeidžiamas vietas:

11.3.1.1. analizuoja taikomųjų programų funkcinius reikalavimus VRKIS, paruošia taikomųjų programų projekto dokumentaciją;

11.3.1.2. atlieka taikomųjų programų testavimo darbus;

11.3.1.3. diegia ir konfigūruoja taikomąsias programas;

diegia papildomus programinius modulius, reikalingus taikomųjų programų veikimui;

11.3.2. pagal kompetenciją techninėmis ir programinėmis priemonėmis užtikrina VRKIS elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą;

11.3.3. techninėmis ir programinėmis priemonėmis registruoja VRKIS elektroninės informacijos saugos incidentus ir informuoja apie juos VRKIS saugos įgaliotinį, teikia VRKIS tvarkytojui pasiūlymus dėl šių incidentų pasekmių pašalinimo;

11.3.4. dalyvauja valdant VRKIS pokyčius, pagal kompetenciją juos įgyvendina;

11.3.5. vykdo VRKIS saugos įgaliotinio nurodymus ir pavedimus, susijusius su VRKIS saugos užtikrinimu;

11.3.6. atlieka kitas VRKIS saugos politiką įgyvendinančiuose dokumentuose nustatytas administratoriaus funkcijas.

12. Teisės aktai, kuriais vadovaujantis tvarkoma VRKIS elektroninė informacija ir užtikrinamas jos saugumas:

12.1. 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB;

12.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

12.3. Lietuvos Respublikos kibernetinio saugumo įstatymas;

12.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

12.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas ir Saugos dokumentų turinio gairių aprašas, patvirtinti 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“;

12.6. 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“;

12.7. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašas, patvirtintas 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“;

12.8. Bendrieji reikalavimai organizacinėms ir techninėms asmens duomenų saugumo priemonėms, patvirtinti Valstybinės 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“;

12.9. Lietuvos standartai LST EN ISO/IEC 27001, LST EN ISO / IEC 27002, taip pat kiti Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo technika“ grupės standartai, apibūdinantys informacijos saugos valdymą ir saugų duomenų tvarkymą;

12.10. kiti teisės aktai, reglamentuojantys informacinių sistemų elektroninės informacijos tvarkymą, elektroninės informacijos saugą, kibernetinį saugumą ir informacinių sistemų valdytojo ir tvarkytojo veiklą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

13. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Klasifikavimo gairių aprašas), 8.1 ir 8.2 papunkčiais, VRKIS tvarkoma elektroninė informacija priskiriama svarbios elektroninės informacijos kategorijai.

14. Vadovaujantis Klasifikavimo gairių aprašo 12.2 papunkčio nuostatomis ir atsižvelgiant į apdorojamos informacijos svarbą, VRKIS priskiriama antrosios kategorijos informacinėms sistemoms.

15. Vadovaujantis Bendrųjų reikalavimų saugumo priemonėms 11.2 papunkčiu, VRKIS organizacinės ir techninės asmens duomenų saugumo priemonės turi užtikrinti antrąjį automatiniu būdu tvarkomų asmens duomenų saugumo lygį.

16. VRKIS saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija.

Saugumo technika“ grupės standartus, ne rečiau kaip kartą per vienus metus organizuoja VRKIS rizikos įvertinimą. Prireikus VRKIS saugos įgaliotinis gali organizuoti neeilinį rizikos įvertinimą. VRKIS rizikos veiksnių vertinimui taikoma kokybinė rizikos vertinimo metodika.

17. VRKIS rizikos įvertinimas išdėstomas rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausieji rizikos veiksniai yra šie:

17.1. 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);

17.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis VRKIS duomenims gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, 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. VRKIS valdytojo vadovas, atsižvelgdamas į VRKIS rizikos įvertinimo ataskaitą, prireikus tvirtina VRKIS saugos įgaliotinio parengtą rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

19. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas VRKIS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

20. Siekiant užtikrinti Nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose išdėstytų nuostatų įgyvendinimo kontrolę, VRKIS saugos įgaliotinis ne rečiau kaip kartą per vienus metus organizuoja VRKIS informacinių technologijų saugos reikalavimų atitikties vertinimą, kurio metu:

20.1. įvertinama Nuostatų ir kitų saugos politiką įgyvendinančių dokumentų atitiktis realiai VRKIS duomenų saugos situacijai;

20.2. inventorizuojama VRKIS valdytojo kompiuterinė techninė ir programinė įranga;

20.3. tikrinama VRKIS tarnybinėse stotyse bei ne mažiau kaip 10 procentų VRKIS valdytojo kompiuterizuotose darbo vietose įdiegta programinė įranga ir jos sąranka (konfigūracija);

20.4. peržiūrima VRKIS naudotojams suteiktų teisių ir atliekamų funkcijų atitiktis, prireikus VRKIS naudotojų teisės praplečiamos arba apribojamos;

20.5. tikrinamos VRKIS duomenų gavėjams suteiktos teisės;

20.6. įvertinamas pasirengimas atkurti VRKIS veiklos tęstinumą, įvykus VRKIS duomenų saugos incidentui.

21. Remdamasis atlikto VRKIS informacinių technologijų saugos reikalavimų atitikties vertinimo rezultatais, VRKIS saugos įgaliotinis parengia ir VRKIS valdytojo vadovui pateikia tvirtinti pastebėtų trūkumų šalinimo planą, kuriame nurodomi atsakingi vykdytojai ir nustatomi numatytų priemonių įgyvendinimo terminai.

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

23. Techninės, programinės ir organizacinės elektroninės informacijos saugos priemonės pasirenkamos, kad būtų užtikrintas VRKIS veiklos tęstinumas patiriant kuo mažiau išlaidų ir užtikrinamas saugus VRKIS naudotojų darbas atsižvelgiant į Lietuvos standarto LST EN ISO / IEC 27002 rekomendacijas.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

24. Programinės įrangos, skirtos apsaugoti VRKIS nuo kenksmingos programinės įrangos (virusų, šnipinėjimui skirtos programinės įrangos ir panašiai) naudojimo nuostatos:

24.1. tarnybinėse stotyse ir kompiuterizuotose darbo vietose naudojamos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės, kurios:

24.1.1. nuolat ieško ir blokuoja kenksmingą programinę įrangą (virusų, šnipinėjimo programinę įrangą ir kita);

24.1.2. kenksmingos programinės įrangos parašai ir paieškos variklis reguliariai atnaujinamas kas 8 val. automatiniu būdu arba inicijavus administratoriui iš centrinės valdymo sistemos;

24.2. tarnybinės stotys ir kompiuterizuotose darbo vietos negali būti eksploatuojamos be kenksmingos programinės įrangos aptikimo priemonių, nebent rizikos vertinimo metu nustatyta, kad esama rizika priimtina.

25. VRKIS kompiuterinis tinklas nuo viešojo interneto turi būti atskirtas filtravimo įranga. Tinklo srautas tarp VRKIS ir viešojo interneto turi būti analizuojamas.

26. Jeigu VRKIS administruoti yra reikalinga naudoti nešiojamąją kompiuterinę įrangą (nešiojamuosius kompiuterius, išorines duomenų laikmenas ir panašiai), tokią įrangą leidžiama laikyti tik institucijos, kuriai pavesta vykdyti VRKIS techninės ir programinės įrangos priežiūrą, patalpose ir naudoti tik VRKIS administravimo tikslu.

27. Naudotojams VRKIS teikia viešą VRKIS tvarkomą informaciją, VRKIS informacija teikiama ir gaunama iš naudotojų, kurie save autentifikavo per Valstybės informacinių išteklių sąveikumo platformą. Iš VRKIS duomenų teikėjų ir VRKIS duomenų šaltinių gaunamų duomenų vientisumas užtikrinamas naudojant viešojo rakto infrastruktūros priemones, kurios leidžia autentifikuoti VRKIS gaunamus duomenis teikiančias kitų informacinių sistemų tarnybines stotis.

28. VRKIS saugiam elektroninės informacijos perdavimui naudojamas saugus šifruotas kanalas, virtualus privatus tinklas (angl. *Virtual Private Network*).

29. VRKIS elektroninės informacijos atsarginės kopijos daromos automatiškai. Periodiškai atliekama atsarginių kopijų tinkamumo ir saugojimo kontrolė. Elektroninės informacijos kopijos turi būti saugomos kitoje patalpoje, negu yra VRKIS tarnybinės stotys.

IV SKYRIUS
PERSONALUI TAIKOMI REIKALAVIMAI

30. VRKIS saugos įgaliotinis privalo turėti atitinkamą kvalifikaciją, išmanyti informacijos saugos užtikrinimo principus, savo darbe vadovautis saugos reikalavimais bei kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą, standartais ir kitais dokumentais, sugebėti prižiūrėti, kaip įgyvendinama saugos politika.

31. VRKIS 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. VRKIS administratoriai privalo sugebėti užtikrinti techninės ir programinės įrangos nepertraukiamą funkcionavimą, stebėti techninės ir programinės įrangos veikimą, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, trikdžių diagnostiką ir šalinimą.

33. VRKIS naudotojai privalo išmanyti Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymą ir kitus teisės aktus, reglamentuojančius asmens duomenų tvarkymą, būti

susipažinę su saugų VRKIS elektroninės informacijos tvarkymą reglamentuojančiais saugos dokumentais.

34. VRKIS naudotojai privalo turėti atitinkamą kvalifikaciją, būti išklausę VRKIS programinės įrangos vartotojų mokymus, pradinį saugaus darbo su duomenimis mokymą ir turėti darbo su *Windows* operacinėmis sistemomis ir taikomosiomis programomis patirties, būti pasirašę pasižadėjimą saugoti asmens duomenų ir kitą VRKIS elektroninę informacijos paslaptį.

35. VRKIS naudotojams ne rečiau kaip kartą per metus turi būti rengiami elektroninės informacijos saugos mokymai, įvairiais būdais primenama apie saugos problematiką (pvz., priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės ir pan.).

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

36. Tvarkyti VRKIS elektroninę informaciją gali tik VRKIS naudotojai, susipažinę su šiais nuostatais, VRKIS saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją užtikrinant jos saugumą, atsakomybe už saugos dokumentų nuostatų pažeidimus ir raštu sutikę laikytis saugos dokumentuose nustatytų reikalavimų. Pakartotinai supažindinama su VRKIS saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais jiems pasikeitus.

37. Už VRKIS naudotojų supažindinimą su šiais nuostatais ir VRKIS saugos politiką įgyvendinančiais dokumentais yra atsakingas VRKIS saugos įgaliotinis.

38. VRKIS naudotojams turi būti nuolat rengiami duomenų saugos mokymai, įvairiais būdais primenama apie saugos problematiką (pvz., priminimai elektroniniu būdu, teminių seminarų rengimas ir panašiai). Už saugumo problemų priminimą, mokymų organizavimą atsako VRKIS saugos įgaliotinis.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

39. Nuostatai ne rečiau kaip kartą per vienus metus arba įvykus esminiams pokyčiams turi būti peržiūrimi.

40. VRKIS administratoriai, VRKIS saugos įgaliotinis, VRKIS naudotojai, VRKIS paslaugų teikėjai, pažeidę VRKIS elektroninės informacijos saugą reglamentuojančių dokumentų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

_____