



**VALSTYBĖS TARNYBOS DEPARTAMENTO
DIREKTORIUS**

Į S A K Y M A S

**DĖL VALSTYBĖS TARNAUTOJŲ REGISTRO IR VALSTYBĖS TARNYBOS VALDYMO
INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO**

2015 m. gruodžio 30 d. Nr. 27V-157
Vilnius

Vadovaudamasis 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 7.1 papunkčiu, 11, 12, ir 19 punktais:

1. Tvirtinu Valstybės tarnautojų registro ir Valstybės tarnybos valdymo informacinės sistemos duomenų saugos nuostatus (pridedama).

2. S k i r i u Valstybės tarnybos departamento Registro ir informacinių sistemų skyriaus vyriausiąjį specialistą Andrių Urmoną Valstybės tarnautojų registro ir Valstybės tarnybos valdymo informacinės sistemos saugos įgaliotiniu.

3. P a v e d u Valstybės tarnautojų registro ir Valstybės tarnybos valdymo informacinės sistemos saugos įgaliotiniui per 6 mėnesius nuo Valstybės tarnautojų registro ir Valstybės tarnybos valdymo informacinės sistemos duomenų saugos nuostatų patvirtinimo parengti ir pateikti Valstybės tarnybos departamento direktoriui tvirtinti Valstybės tarnautojų registro ir Valstybės tarnybos valdymo informacinės sistemos saugos politiką įgyvendinančių dokumentų projektus.

4. P r i p a ž i s t u netekusiais galios:

4.1. Valstybės tarnybos departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2005 m. lapkričio 21 d. įsakymą Nr. 27V-76 „Dėl Valstybės tarnautojų registro duomenų saugos nuostatų patvirtinimo“ su visais jo pakeitimais ir papildymais;

4.2. Valstybės tarnybos valdymo informacinės sistemos duomenų saugos nuostatus, patvirtintus Valstybės tarnybos departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2007 m. sausio 8 d. įsakymu Nr. 27V-8 „Dėl Valstybės tarnybos valdymo informacinės sistemos nuostatų ir Valstybės tarnybos valdymo informacinės sistemos duomenų saugos nuostatų patvirtinimo“, su visais jų pakeitimais ir papildymais.

Direktorius

Osvaldas Šarmavičius

SUDERINTA

Lietuvos Respublikos vidaus reikalų ministerijos
2015 m. gruodžio 9 d. raštu Nr. 1D-9632

VALSTYBĖS TARNAUTOJŲ REGISTRO IR VALSTYBĖS TARNYBOS VALDYMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS BENDROSIOS NUOSTATOS

1. Valstybės tarnautojų registro ir Valstybės tarnybos valdymo informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato Valstybės tarnautojų registro (toliau – VATARAS) ir Valstybės tarnybos valdymo informacinės sistemos (toliau – VATIS) elektroninės informacijos saugos politiką, organizacines, technines, programines, teisinės ir kitas priemones, užtikrinančias saugų VATARAS ir VATIS elektroninės informacijos tvarkymą.

2. Saugos nuostatuose vartojamos sąvokos apibrėžtos 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ (toliau – Saugos reikalavimų aprašas).

3. VATARAS ir VATIS elektroninės informacijos saugos politika įgyvendinama pagal VATARAS ir VATIS valdytojo tvirtinamus VATARAS ir VATIS saugos politiką įgyvendinančius dokumentus:

3.1. Valstybės tarnautojų registro ir Valstybės tarnybos valdymo informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės;

3.2. Valstybės tarnautojų registro ir Valstybės tarnybos valdymo informacinės sistemos veiklos tęstinumo valdymo planą;

3.3. Valstybės tarnautojų registro ir Valstybės tarnybos valdymo informacinės sistemos naudotojų administravimo taisyklės.

4. VATARAS ir VATIS elektroninės informacijos saugumo užtikrinimo tikslas – sudaryti sąlygas saugiai automatinio būdu tvarkyti VATARAS ir VATIS elektroninę informaciją, užtikrinti VATARAS ir VATIS elektroninės informacijos konfidencialumą, prieinamumą, vientisumą ir tinkamą techninės ir programinės įrangos funkcionavimą.

5. VATARAS ir VATIS elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

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

5.2. VATARAS ir VATIS elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

5.3. VATARAS ir VATIS tvarkomų asmens duomenų apsauga;

5.4. VATARAS ir VATIS veiklos tęstinumo užtikrinimas.

6. VATARAS ir VATIS elektroninės informacijos saugai užtikrinti kompleksiskai naudojamos organizacinės, teisinės, techninės ir programinės priemonės.

7. Saugos nuostatai taikomi VATARAS ir VATIS valdytojui, VATARAS ir VATIS tvarkytojams, VATARAS ir VATIS saugos įgaliotiniui, VATARAS ir VATIS administratoriams, VATARAS ir VATIS naudotojams.

8. VATARAS ir VATIS valdytojas – Valstybės tarnybos departamentas (toliau – Departamentas), Labdarių g. 8, LT-01120 Vilnius, atlieka Valstybės tarnautojų registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2002 m. rugpjūčio 10 d. nutarimu Nr. 1255 „Dėl Valstybės tarnautojų registro nuostatų patvirtinimo“ (toliau – VATARAS nuostatai) ir Valstybės tarnybos valdymo informacinės sistemos nuostatuose, patvirtintuose Valstybės tarnybos departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2007 m. sausio 8 d. įsakymu Nr. 27V-8 „Dėl Valstybės tarnybos valdymo informacinės sistemos nuostatų ir Valstybės tarnybos valdymo informacinės sistemos duomenų saugos nuostatų patvirtinimo“ (toliau – VATIS nuostatai), apibrėžtas funkcijas, o taip pat:

8.1. atsako už saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą;

8.2. tvirtina VATARAS ir VATIS saugos politiką įgyvendinančius dokumentus, kitus dokumentus, susijusius su elektroninės informacijos sauga, ir jų pakeitimus;

8.3. prižiūri ir kontroliuoja, kad VATARAS ir VATIS būtų tvarkoma vadovaujantis Lietuvos Respublikos įstatymais, VATARAS nuostatais, VATIS nuostatais, Saugos nuostatais, VATARAS ir VATIS saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais;

8.4. priima sprendimus dėl VATARAS ir VATIS techninių ir programinių priemonių, būtinų VATARAS ir VATIS elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

8.5. nagrinėja VATARAS ir VATIS tvarkytojų pasiūlymus dėl VATARAS ir VATIS saugos tobulinimo ir priima dėl jų sprendimus;

8.6. priima sprendimą dėl VATARAS ir VATIS informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

8.7. vykdo kitas Saugos nuostatais, VATARAS nuostatais, VATIS nuostatais, Saugos reikalavimų aprašu ir kitais teisės aktais, reglamentuojančiais VATARAS ir VATIS elektroninės informacijos tvarkymo teisėtumą ir saugos valdymą, priskirtas funkcijas.

9. VATARAS ir VATIS tvarkytojai – Departamentas ir kitos valstybės ir savivaldybių institucijos ir įstaigos (toliau – įstaigos), nurodytos Valstybės tarnybos įstatymo 2 straipsnio 4 dalyje, elektroniniu būdu tvarkančios VATARAS ir VATIS duomenis.

10. Departamentas, kaip VATARAS ir VATIS tvarkytojas, atlieka VATARAS nuostatuose ir VATIS nuostatuose nustatytas funkcijas, o taip pat:

10.1. užtikrina tinkamą VATARAS ir VATIS valdytojo patvirtintų Saugos nuostatų, VATARAS ir VATIS saugos politiką įgyvendinančių dokumentų, kitų dokumentų, susijusių su elektroninės informacijos sauga, ir rekomendacijų įgyvendinimą;

10.2. skiria VATARAS ir VATIS saugos įgaliotinį ir VATARAS ir VATIS administratorius;

10.3. atlieka kitas Saugos nuostatų, Saugos reikalavimų aprašo, VATARAS nuostatų, VATIS nuostatų ir kitų teisės aktų nustatytas funkcijas, susijusias su VATARAS ir VATIS elektroninės informacijos sauga.

11. Įstaigos, nurodytos Saugos nuostatų 9 punkte, kaip VATARAS ir VATIS tvarkytojai, atlieka VATARAS nuostatuose ir VATIS nuostatuose nustatytas funkcijas, o taip pat:

11.1. vadovaudamosi Saugos nuostatais, Valstybės tarnautojų registro ir Valstybės tarnybos valdymo informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėmis, Valstybės tarnautojų registro ir Valstybės tarnybos valdymo informacinės sistemos naudotojų administravimo taisyklėmis tvarko VATARAS ir VATIS elektroninę informaciją;

11.2. užtikrina VATARAS ir VATIS elektroninės informacijos tvarkymo teisėtumą;

11.3. informuoja VATARAS ir VATIS saugos įgaliotinį, VATARAS ir VATIS administratorius apie elektroninės informacijos saugos incidentus, VATARAS ir VATIS darbo sutrikimus;

11.4. vykdo kitas Saugos nuostatuose ir VATARAS ir VATIS saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas ir kitus Departamento direktoriaus, VATARAS ir VATIS saugos įgaliotinio ir VATARAS ir VATIS administratorių nurodymus, susijusius su VATARAS ir VATIS elektroninės informacijos sauga;

11.5. užtikrina tvarkomos VATARAS ir VATIS elektroninės informacijos saugą VATARAS ir VATIS tvarkytojo įstaigoje. VATARAS ir VATIS tvarkytojų vadovai atsako už reikiamų organizacinių, techninių ir programinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir VATARAS ir VATIS saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka.

12. VATARAS ir VATIS saugos įgaliotinis koordinuoja ir prižiūri VATARAS ir VATIS elektroninės informacijos saugos politikos įgyvendinimą ir atlieka kitas funkcijas:

12.1. teikia Departamento direktoriui siūlymus dėl:

12.1.1. Saugos nuostatų ir VATARAS ir VATIS saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar pripažinimo netekus galios;

12.1.2. VATARAS ir VATIS informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

12.2. organizuoja VATARAS ir VATIS rizikos įvertinimą;

12.3. koordinuoja elektroninės informacijos saugos incidentų tyrimą;

12.4. teikia VATARAS ir VATIS administratoriams, VATARAS ir VATIS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su VATARAS ir VATIS saugos politikos įgyvendinimu;

12.5. periodiškai, ne rečiau kaip kartą per kalendorinius metus, organizuoja VATARAS ir VATIS administratorių bei VATARAS ir VATIS naudotojų saugos mokymus, reguliariai jiems primena saugos problemas, teikia konsultacijas;

12.6. užtikrina, kad VATARAS ir VATIS naudotojai susipažintų su Saugos nuostatais ir VATARAS ir VATIS saugos politiką įgyvendinančiais dokumentais bei atsakomybe už šių reikalavimų nesilaikymą.

12.7. atlieka kitas Saugos nuostatų, VATARAS nuostatų, VATIS nuostatų, Saugos reikalavimų aprašo ir kitų teisės aktų nustatytas funkcijas.

13. VATARAS ir VATIS priežiūrą atlieka VATARAS ir VATIS administratoriai: VATARAS ir VATIS komponentų administratorius, duomenų perdavimo administratorius, duomenų bazių ir naudotojų administratorius:

13.1. VATARAS ir VATIS komponentų administratoriaus funkcijos ir atsakomybė:

13.1.1. užtikrina VATARAS ir VATIS funkcionavimą;

13.1.2. atsako už VATARAS ir VATIS komponentų (tarnybinių stočių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, įsilaužimo aptikimo sistemų, bylų serverių) administravimą;

13.2. duomenų perdavimo administratoriaus funkcijos ir atsakomybė:

13.2.1. atsako už saugų VATARAS ir VATIS duomenų ir elektroninės informacijos perdavimą tinklais;

13.2.2. organizuoja VATARAS ir VATIS komponentų sąrankos aprašo dokumentacijos parengimą ir atnaujinimą, pažeidžiamų vietų nustatymą ir saugos priemonių parinkimą bei jų atitiktį Saugos nuostatų ir VATARAS ir VATIS saugos politiką įgyvendinančių dokumentų reikalavimams;

13.3. duomenų bazių ir naudotojų administratoriaus funkcijos ir atsakomybė:

13.3.1. kuria ir administruoja VATARAS ir VATIS naudotojų registracijos į duomenų bazes duomenis;

13.3.2. atsako už VATARAS ir VATIS duomenų konfidencialumą ir vientisumą;

13.3.3. analizuoja VATARAS ir VATIS naudotojų veiksmų registracijos žurnalų įrašus;

13.4. Bendros VATARAS ir VATIS administratorių funkcijos ir atsakomybė:

13.4.1. pagal kompetenciją atlieka VATARAS ir VATIS saugumo reikalavimų atitikties nustatymą ir stebėseną;

13.4.2. nuolat teikia VATARAS ir VATIS saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę;

13.4.3. pagal kompetenciją rengia pasiūlymus dėl VATARAS ir VATIS palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

13.4.4. registruoja elektroninės informacijos saugos incidentus, informuoja apie juos VATARAS ir VATIS saugos įgaliotinį ir teikia pasiūlymus dėl minėtų incidentų pašalinimo;

13.4.5. vykdo kitas Saugos nuostatuose ir VATARAS ir VATIS saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas ir kitus Departamento direktoriaus ar VATARAS ir VATIS saugos įgaliotinio nurodymus, susijusius su VATARAS ir VATIS sauga.

14. Teisės aktai, kuriais vadovaujantis tvarkomi VATARAS ir VATIS duomenys ir užtikrinama jų sauga:

14.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

14.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

14.3. Lietuvos Respublikos kibernetinio saugumo įstatymas;

14.4. Lietuvos standartai LST ISO/IEC 27001:2013, LST ISO/IEC 27002:2014 bei kiti Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, reglamentuojantys saugų duomenų tvarkymą;

14.5. 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“;

14.6. Saugos reikalavimų aprašas;

14.7. Saugos dokumentų turinio gairių aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

14.8. Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

14.9. 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“ (toliau – Bendrieji reikalavimai organizacinėms ir techninėms asmens duomenų saugumo priemonėms);

14.10. kiti saugos politiką įgyvendinantys dokumentai.

II SKYRIUS

ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

15. VATARAS ir VATIS tvarkoma elektroninė informacija priskirtina svarbios elektroninės informacijos kategorijai, vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, (toliau – Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas) 4.2.4 ir 4.2.7 papunkčių nuostatomis.

16. Atsižvelgiant į VATARAS ir VATIS apdorojamos elektroninės informacijos svarbos kategoriją, VATARAS ir VATIS priskiriama antrajai kategorijai vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo, 5.2 papunkčio nuostatomis.

17. VATARAS ir VATIS asmens duomenų tvarkymas automatinio būdu priskirtinas antrajam saugumo lygiui, vadovaujantis Bendrųjų reikalavimų organizacinėms ir techninėms asmens duomenų saugumo priemonėms 11.2 papunkčio nuostatomis.

18. VATARAS ir VATIS saugos įgaliotinis, atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja VATARAS ir VATIS rizikos įvertinimą ir parengia VATARAS ir VATIS rizikos įvertinimo ataskaitą. Prireikus VATARAS ir VATIS saugos įgaliotinis gali organizuoti neeilinį VATARAS ir VATIS rizikos įvertinimą.

19. VATARAS ir VATIS rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnus, galinčius turėti įtakos informacijos saugai. Svarbiausieji rizikos veiksniai yra šie:

19.1. subjektyvūs netyčiniai (duomenų tvarkymo klaidos ir apsirikimai, duomenų ištrynimasis, klaidingas duomenų teikimas, duomenų perdavimo tinklų veiklos sutrikimai, programinės įrangos klaidos, netinkamas veikimas ir kita);

19.2. subjektyvūs tyčiniai (nesankcionuotas naudojimas VATARAS ir VATIS duomenims gauti, duomenų pakeitimas ar sunaikinimas, duomenų perdavimo tinklų veiklos trikdymai, saugos pažeidimai, vagystės ir kita);

19.3. 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.

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

21. Siekdamas užtikrinti Saugos nuostatuose ir VATARAS ir VATIS saugos politiką įgyvendinančiuose dokumentuose nustatytų reikalavimų įgyvendinimo organizavimą ir kontrolę, VATARAS ir VATIS saugos įgaliotinis ne rečiau kaip kartą per metus organizuoja VATARAS ir VATIS informacinių technologijų saugos reikalavimų atitikties vertinimą, kurio metu:

21.1. įvertinama realios VATARAS ir VATIS elektroninės informacijos saugos situacijos atitiktis Saugos nuostatų, VATARAS ir VATIS saugos politiką įgyvendinančių dokumentų ir kitų teisės aktų reikalavimams;

21.2. patikrinama ne mažiau kaip 10 VATARAS ir VATIS naudotojų kompiuterizuotų darbo vietų ir VATARAS ir VATIS tarnybinėse stotyse įdiegta programinė įranga bei jos sąranka;

21.3. patikrinama VATARAS ir VATIS naudotojams ir VATARAS ir VATIS administratoriams suteiktų teisių tvarkyti VATARAS ir VATIS atitiktis atliekamoms funkcijoms, prireikus VATARAS ir VATIS naudotojų teisės praplečiamos ar apribojamos;

21.4. įvertinamas pasiruošimas užtikrinti VATARAS ir VATIS veiklos tęstinumą įvykus elektroninės informacijos saugos incidentui;

22. Remdamasis atlikto VATARAS ir VATIS informacinių technologijų saugos reikalavimų atitikties vertinimo rezultatais, VATARAS ir VATIS saugos įgaliotinis parengia ir Departamento direktoriui pateikia tvirtinti pastebėtų trūkumų šalinimo planą, kuriame nurodomi atsakingi vykdytojai ir nustatomi numatytųjų priemonių įgyvendinimo terminai.

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. VATARAS ir VATIS tarnybinėse stotyse ir kompiuterizuotose darbo vietose turi būti naudojamos kenksmingos programinės įrangos aptikimo priemonės, nuolat ieškančios ir blokuojančios kenksmingą programinę įrangą (virusų, šnipinėjimo programinę įrangą ir kt.), kurios turi būti reguliariai atnaujinamos automatinio būdu ne rečiau kaip kartą per 48 valandas.

25. Programinės įrangos, įdiegtos VATARAS ir VATIS tarnybinėse stotyse ir kompiuterizuotose darbo vietose, naudojimo nuostatos:

25.1. VATARAS ir VATIS darbui turi būti naudojama tik legali programinė įranga;

25.2. programinė įranga atnaujinama laikantis gamintojo reikalavimų;

25.3. VATARAS ir VATIS tarnybinėse stotyse neturi veikti programinė įranga, nesusijusi su VATARAS ir VATIS duomenų tvarkymu, VATARAS ir VATIS naudotojų ir pačios įrangos administravimu;

25.4. VATARAS ir VATIS programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims;

25.5. VATARAS ir VATIS saugos įgaliotinis parengia ir suderina su VATARAS ir VATIS valdytojo vadovu leistinos programinės įrangos sąrašą, kurį kiekvienais metais peržiūri bei prireikus atnaujiną;

26. VATARAS ir VATIS tarnybinių stočių kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kt.) pagrindinės naudojimo nuostatos:

26.1. kompiuterių tinklai nuo viešųjų telekomunikacijų tinklų (interneto) turi būti atskirti ugniasienėmis, DOS ir DDOS atakų prevencijai skirta įranga bei įsilaužimų aptikimo ir prevencijos įranga;

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

26.3. naudojamos turinio filtravimo sistemos.

27. Metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą:

27.1. VATARAS ir VATIS naudotojų, jų vykdytų užklausų ir peržiūrėtų užklausų rezultatų duomenys tvarkomi VATARAS ir VATIS administratoriaus posistemėse Departamento direktoriaus nustatyta tvarka.

27.2. Tiesioginė prieiga prie VATARAS ir VATIS duomenų suteikiama įgyvendinus VATARAS ir VATIS naudotojų autentifikavimo priemones. Tiesioginė prieiga prie VATARAS ir VATIS duomenų užtikrinama automatinio būdu ištisą parą darbo ir poilsio dienomis.

27.3. VATARAS ir VATIS duomenys perduodami automatinio būdu naudojant TCP/IP protokolą realia laike (*On-line* režimu) arba asinchroniniu režimu pagal VATARAS ir VATIS duomenų teikimo sutartis, kuriose nustatytos perduodamų duomenų specifikacijos, kopijų skaičius, kitos duomenų perdavimo sąlygos ir tvarka.

27.4. VATARAS ir VATIS duomenys, perduodami ne per Saugų valstybinį duomenų perdavimo tinklą ir ne per Vidaus reikalų telekomunikacinį tinklą, turi būti šifruojami; duomenų šifravimą privalo užtikrinti VATARAS ir VATIS valdytojas; VATARAS ir VATIS duomenų gavėjų prieigą prie VATARAS ir VATIS duomenų turi kontroliuoti tinklo užkarda.

28. VATARAS ir VATIS naudotojams, savo tarnybinėms funkcijoms vykdyti naudojantiems nešiojamuosius kompiuterius VATARAS ir VATIS duomenų perdavimui kompiuterių tinklais ne savo darbo vietoje, šiuose kompiuteriuose turi būti naudojamas kompiuterio įjungimo slaptažodis, papildomas VATARAS ir VATIS naudotojo tapatybės patvirtinimas ir VATARAS ir VATIS elektroninės informacijos šifravimas.

29. VATARAS ir VATIS naudotojams, kuriems būtinas prisijungimas tiesioginėms pareigoms atlikti iš nutolusios darbo vietos, gali būti suteikiama nuotolinio prisijungimo prie VATARAS ir VATIS galimybė:

29.1. techninis nuotolinio prisijungimo sprendimas turi užtikrinti ne žemesnį nei vidiniam prisijungimui naudojamą saugumo lygį, t. y. turi būti naudojamos Saugos nuostatuose nurodytos priemonės ir elektroninės informacijos šifravimas naudojantis virtualiu privačiu tinklu (angl. *virtual private network* – VPN);

29.2. prie VATARAS ir VATIS prisijungiama nuotoliniu būdu naudojant interneto naršyklę (HTTPS protokolą).

30. Pagrindiniai atsarginių elektroninės informacijos kopijų darymo ir atkūrimo reikalavimai:

30.1. VATARAS ir VATIS elektroninės informacijos kopijos turi būti daromos automatiškai kiekvieną dieną. Prireikus jas atkurti turi teisę VATARAS ir VATIS administratorius;

30.2. atkūrimas iš elektroninės informacijos kopijų privalo būti išbandomas ne rečiau kaip 2 kartus per metus;

30.3. elektroninės informacijos kopijos turi būti saugomos kitoje patalpoje nei VATARAS ir VATIS tarnybinės stotys. Elektroninė informacija kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, neleidžiančių panaudoti kopijas neteisėtai atkurti elektroninę informaciją.

IV SKYRIUS REIKALAVIMAI PERSONALUI

31. VATARAS ir VATIS saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, tobulinti kvalifikaciją elektroninės informacijos saugos srityje, savo darbe vadovautis Saugos reikalavimų aprašo, kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis, turėti darbo su duomenų bazėmis, operacinėmis sistemomis, taikomosiomis programomis patirties.

32. VATARAS ir VATIS 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.

33. VATARAS ir VATIS administratoriai privalo išmanyti pagrindinius saugos politikos principus, darbą su duomenų perdavimo tinklais, mokėti užtikrinti jų saugumą, turėti sisteminių programinių priemonių (Windows, Unix) administravimo bei priežiūros patirties, turi būti susipažinęs su Saugos nuostatais ir VATARAS ir VATIS saugos politiką įgyvendinančiais dokumentais, taip pat kitomis vidaus ir darbo saugos taisyklėmis.

34. VATARAS ir VATIS naudotojai privalo turėti darbo kompiuteriu įgūdžių. Tvarkyti VATARAS ir VATIS duomenis gali tik VATARAS ir VATIS naudotojai, susipažinę su Saugos nuostatais ir VATARAS ir VATIS saugos politiką įgyvendinančiais dokumentais.

35. VATARAS ir VATIS naudotojams turi būti nuolat rengiami duomenų saugos mokymai, įvairiais būdais primenama apie saugos problematiką (pvz., priminimai elektroniniu būdu, teminių seminarų rengimas, atmintinės priimtiems naujiems darbuotojams ir pan.).

V SKYRIUS

VATARAS IR VATIS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

36. VATARAS ir VATIS naudotojai su Saugos nuostatais ir VATARAS ir VATIS saugos politiką įgyvendinančiais dokumentais ir atsakomybe už šių reikalavimų nesilaikymą susipažįsta ir patvirtina apie susipažinimą jungdamiesi prie VATARAS ir VATIS per naudotojo sąsają. VATARAS ir VATIS saugos įgaliotinis per VATARAS ir VATIS sistemą informuoja VATARAS ir VATIS naudotojus apie Saugos nuostatų pakeitimus ar kitų saugos politiką įgyvendinančių teisės aktų pripažinimą netekusiais galios, keitimą ar priėmimą.

37. VATARAS ir VATIS naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veiklos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti VATARAS ir VATIS saugos įgaliotiniui ir/arba VATARAS ir VATIS administratoriams.

38. Esant elektroninės informacijos saugos incidentui, nenumatytai situacijai, VATARAS ir VATIS saugos įgaliotinio, VATARAS ir VATIS administratorių, VATARAS ir VATIS naudotojų veiksmus reglamentuoja Valstybės tarnautojų registro ir Valstybės tarnybos valdymo informacinės sistemos veiklos tęstinumo valdymo planas.

VI SKYRIUS

BAIGIAMOSIOS NUOSTATOS

39. VATARAS ir VATIS saugos įgaliotinis, VATARAS ir VATIS administratoriai, VATARAS ir VATIS naudotojai, pažeidę Saugos nuostatų ar kitų saugos politiką įgyvendinančių teisės aktų reikalavimus, atsako Lietuvos Respublikos įstatymų ir kitų teisės aktų nustatyta tvarka.
