Įsakymas netenka galios 2020-04-01:
Valstybės tarnybos departamentas, Įsakymas
Nr. 27V-28, 2020-03-27, paskelbta TAR 2020-03-31, i. k. 2020-06657
Dėl kai kurių Valstybės tarnybos departamento direktoriaus įsakymų pripažinimo netekusiais galios

Suvestinė redakcija nuo 2018-04-18 iki 2020-03-31

Įsakymas paskelbtas: TAR 2015-12-30, i. k. 2015-21070

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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 7.1 papunkčiu, 11, 12, ir 19 punktais ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo, patvirtinto 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“, 5 punktu:
Preambulės pakeitimai:
Nr. 27V-65, 2018-04-16, paskelbta TAR 2018-04-17, i. k. 2018-06160

1. T v i r t i n u 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. S k i r i u Valstybės tarnybos departamento Registro ir informacinių sistemų skyriaus vedėją Paulių Strišką asmeniu, atsakingu už kibernetinio saugumo organizavimą ir užtikrinimą.
Papildyta punktu:
Nr. 27V-65, 2018-04-16, paskelbta TAR 2018-04-17, i. k. 2018-06160

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

Punkto numeracijos pakeitimas:
Nr. 27V-65, 2018-04-16, paskelbta TAR 2018-04-17, i. k. 2018-06160

5.1. 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;

5.2. 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

PATVIRTINTA
Valstybės tarnybos departamento direktoriaus
2015 m. gruodžio 30 d. įsakymu Nr. 27V-157
(2018 m. balandžio 16 d. įsakymo Nr. 27V-65
redakcija)

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 ir kibernetinio saugumo politiką.

2. Saugos nuostatuose vartojamos sąvokos apibrėžtos 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“ (toliau – Saugos reikalavimų aprašas), Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo, patvirtinto 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“ (toliau – Kibernetinio saugumo reikalavimų aprašas).

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

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

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 taisykles.

4. VATARAS ir VATIS elektroninės informacijos saugumo užtikrinimo tikslas – sudaryti sąlygas saugiai automatiniu 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 saugos ir kibernetinio saugumo užtikrinimo prioritetinės kryptys:

5.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų VATARAS ir VATIS elektroninės informacijos saugai ir kibernetiniam saugumui 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 ir kibernetiniam saugumui užtikrinti kompleksiškai 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 kibernetinio saugumo vadovui, 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 direktoriaus 2007 m. sausio 8 d. įsakymu Nr. 27V-8 „Dėl Valstybės tarnybos valdymo informacinės sistemos nuostatų patvirtinimo“ (toliau – VATIS nuostatai), apibrėžtas funkcijas, o taip pat:

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

8.2. tvirtina VATARAS ir VATIS saugos ir kibernetinio saugumo politiką įgyvendinančius dokumentus, kitus dokumentus, susijusius su elektroninės informacijos sauga ir kibernetinio saugumu, 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 ir kibernetinio saugumo 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 ir kibernetiniam saugumui užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

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

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

8.7. vykdo kitas Saugos nuostatais, VATARAS nuostatais, VATIS nuostatais, Saugos reikalavimų aprašu, Kibernetinio saugumo reikalavimų aprašu ir kitais teisės aktais, reglamentuojančiais VATARAS ir VATIS elektroninės informacijos tvarkymo teisėtumą, saugos ir kibernetinio saugumo 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 ir kibernetinio saugumo politiką įgyvendinančių dokumentų, kitų dokumentų, susijusių su elektroninės informacijos sauga, ir rekomendacijų įgyvendinimą;

10.2. skiria VATARAS ir VATIS saugos įgaliotinį, kibernetinio saugumo vadovą ir VATARAS ir VATIS administratorius;

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

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, kibernetinio saugumo vadovą, VATARAS ir VATIS administratorius apie elektroninės informacijos saugos ir kibernetinio saugumo incidentus, VATARAS ir VATIS darbo sutrikimus;

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

11.5. užtikrina tvarkomos VATARAS ir VATIS elektroninės informacijos saugą ir kibernetinį saugumą VATARAS ir VATIS tvarkytojo įstaigoje. VATARAS ir VATIS tvarkytojų vadovai atsako už reikiamų organizacinių, techninių ir programinių saugos ir kibernetinio saugumo priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir VATARAS ir VATIS saugos ir kibernetinio saugumo 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 kibernetinio saugumo vadovas atlieka Kibernetinio saugumo reikalavimų apraše ir kituose teisės aktuose nustatytas funkcijas. VATARAS ir VATIS kibernetinio saugumo vadovas ir saugos įgaliotinis gali būti tas pats asmuo.

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

14.1. VATARAS ir VATIS komponentų administratoriaus funkcijos ir atsakomybė:

14.1.1. užtikrina VATARAS ir VATIS funkcionavimą;

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

14.2. duomenų perdavimo administratoriaus funkcijos ir atsakomybė:

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

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

14.3. duomenų bazių ir naudotojų administratoriaus funkcijos ir atsakomybė:

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

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

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

14.4. Bendros VATARAS ir VATIS administratorių funkcijos ir atsakomybė:

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

14.4.2. nuolat teikia VATARAS ir VATIS saugos įgaliotiniui ir kibernetinio saugumo vadovui informaciją apie saugą ir kibernetinį saugumą užtikrinančių pagrindinių komponentų būklę;

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

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

14.4.5. vykdo kitas Saugos nuostatuose ir VATARAS ir VATIS saugos ir kibernetinio saugumo politiką įgyvendinančiuose dokumentuose nustatytas funkcijas ir kitus Departamento direktoriaus ar VATARAS ir VATIS saugos įgaliotinio ir kibernetinio saugumo vadovo nurodymus, susijusius su VATARAS ir VATIS sauga ir kibernetiniu saugumu.

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

15.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

15.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

15.3. Lietuvos Respublikos kibernetinio saugumo įstatymas;

15.4. Lietuvos standartai LST ISO/IEC 27001:2017, LST ISO/IEC 27002:2017 bei kiti Lietuvos ir tarptautiniai „Informacinės technologijos. Saugumo metodai“ grupės standartai, reglamentuojantys saugų duomenų tvarkymą;

15.5. 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“;

15.6. Kibernetinio saugumo reikalavimų aprašas;

15.7. Saugos reikalavimų aprašas;

15.8. 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 Elektroninės informacijos, sudarančios valstybės

informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“;

15.9. 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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“;

15.10. 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);

15.11. kiti saugos ir kibernetinio saugumo politiką įgyvendinantys dokumentai.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

16. VATARAS ir VATIS tvarkoma elektroninė informacija priskirtina svarbios elektroninės informacijos kategorijai, 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 – Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas) 8.2 ir 8.3 papunkčių nuostatomis.

17. Atsižvelgiant į VATARAS ir VATIS apdorojamos elektroninės informacijos svarbos kategoriją, VATARAS ir VATIS priskiriama antrajai kategorijai vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, 12.2 papunkčio nuostatomis.

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

19. 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. Kartu su VATARAS ir VATIS rizikos įvertinimu ir (ar) Saugos nuostatų 23 punkte nurodytu informacinių technologijų saugos reikalavimų atitikties vertinimu turi būti atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos VATARAS ir VATIS kibernetiniam saugumui, vertinimas. Prireikus VATARAS ir VATIS saugos įgaliotinis gali organizuoti neeilinį VATARAS ir VATIS rizikos įvertinimą.

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

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

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

20.3. 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.

21. 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.

22. VATARAS ir VATIS valdytojas rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2012 m. spalio 16 d. įsakymu Nr. 1V-740 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“ (toliau – Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatai), nustatyta tvarka.

23. 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 ir atitikties Kibernetinio saugumo reikalavimų apraše nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimą.

24. VATARAS ir VATIS informacinių technologijų saugos atitikties vertinimo metu turi būti atliekamas kibernetinių atakų imitavimas ir vykdomos kibernetinių incidentų imitavimo pratybos.

25. Kibernetinių atakų imitavimas atliekamas šiais etapais:

25.1. planavimo etapas. Parengiamas kibernetinių atakų imitavimo planas, kuriame apibrėžiami kibernetinių atakų imitavimo tikslai ir darbų apimtis, pateikiamas darbų grafikas, aprašomi planuojamų imituoti kibernetinių atakų tipai (išorinės ir (ar) vidinės), kibernetinių atakų imitavimo būdai (juodosios dėžės (angl. *Black Box*), baltosios dėžės (angl. *White Box*) ir (ar) pilkosios dėžės (angl. *Grey Box*)), galima neigiama įtaka veiklai, kibernetinių atakų imitavimo metodologija, programiniai ir (ar) techniniai įrankiai ir priemonės, nurodomi už plano vykdymą atsakingi asmenys ir jų kontaktai. Kibernetinių atakų imitavimo planas turi būti suderintas su Departamento direktoriumi ir vykdomas tik gavus jo rašytinį pritarimą;

25.2. žvalgybos (angl. *Reconnaissance*) ir aptikimo (angl. *Discovery*) etapas. Surenkama informacija apie perimetrą, tinklo mazgus, tinklo mazguose veikiančių tarnybinių stočių ir kitų tinklo įrenginių operacines sistemas ir programinę įrangą, paslaugas (angl. *Services*), pažeidžiamumą, konfigūracijas ir kitą sėkmingai kibernetinei atakai įvykdyti reikalingą informaciją. Šiame etape turi būti teikiamos tarpinės ataskaitos apie vykdomą veiklą ir jos rezultatus;

25.3. kibernetinių atakų imitavimo etapas. Atliekami kibernetinių atakų imitavimo plane numatyti testai. Šiame etape turi būti teikiamos tarpinės ataskaitos apie vykdomas veiklas ir jos rezultatus;

25.4. ataskaitos parengimo etapas. Kibernetinių atakų imitavimo rezultatai turi būti išdėstomi pažeidžiamumų nustatymo ataskaitoje. Kibernetinių atakų imitavimo plane numatyti testų rezultatai turi būti detalizuojami ataskaitoje ir lyginami su planuotais. Kiekvienas aptiktas pažeidžiamumas turi būti detalizuojamas ir pateikiamos rekomendacijos jam pašalinti. Kibernetinių atakų imitavimo rezultatai turi būti pagrįsti patikimais įrodymais ir rizikos įvertimu. Jeigu nustatoma incidentų valdymo ir šalinimo, taip pat organizacijos nepertraukiamos veiklos užtikrinimo trūkumų, turi būti tobulinami veiklos tęstinumo planai.

26. Remdamasis atlikto VATARAS ir VATIS informacinių technologijų saugos reikalavimų atitikties ir atitikties Kibernetinio saugumo reikalavimų apraše nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams 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.

27. Elektroninės informacijos saugos ir kibernetinio saugumo būklė gerinama techninėmis, programinėmis, organizacinėmis ir kitomis VATARAS ir VATIS elektroninės informacijos saugos ir kibernetinio saugumo priemonėmis. Pagrindiniai elektroninės informacijos saugos ir kibernetinio saugumo priemonių parinkimo principai yra šie:

27.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

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

27.3. turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos ir kibernetinio saugumo priemonės.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

28. 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 automatiniu būdu ne rečiau kaip kartą per 48 valandas.

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

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

29.2. programinė įranga, kibernetiniam saugumui užtikrinti naudojamos priemonės atnaujinamos laikantis gamintojo reikalavimų;

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

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

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

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

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

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

30.3. naudojamos turinio filtravimo sistemos.

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

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

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

31.3. VATARAS ir VATIS duomenys perduodami automatiniu būdu naudojant TCP/IP protokolą realiame 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.

31.4. 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.

32. 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.

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

33.1. 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);

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

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

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

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

34.3. 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.

35. VATARAS ir VATIS valdytojas pirkdamas paslaugas, darbus ar įrangą, susijusius su VATARAS ir VATIS, jų projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, iš anksto pirkimo dokumentuose turi nustatyti, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas užtikrina atitiktį Kibernetinio saugumo reikalavimų aprašui.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

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

37. VATARAS ir VATIS saugos įgaliotiniu ir Kibernetinio saugumo vadovu 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.

38. VATARAS ir VATIS administratoriai privalo išmanyti pagrindinius saugos ir kibernetinio saugumo užtikrinimo 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 ir kibernetinio saugumo politiką įgyvendinančiais dokumentais, taip pat kitomis vidaus ir darbo saugos taisyklėmis.

39. 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 ir kibernetinio saugumo politiką įgyvendinančiais dokumentais.

40. VATARAS ir VATIS naudotojams turi būti nuolat rengiami duomenų saugos ir kibernetinio saugumo mokymai, įvairiais būdais primenama apie saugos ir kibernetinio saugumo 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

41. VATARAS ir VATIS naudotojai su Saugos nuostatais ir VATARAS ir VATIS saugos ir kibernetinio saugumo 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 ir kibernetinio saugumo politiką įgyvendinančių teisės aktų pripažinimą netekusiais galios, keitimą ar priėmimą.

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

43. Esant elektroninės informacijos saugos ir kibernetinio saugumo incidentui, nenumatytai situacijai, VATARAS ir VATIS saugos įgaliotinio, Kibernetinio saugumo vadovo, 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

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

Pakeitimai:

1.
Valstybės tarnybos departamentas, Įsakymas
Nr. 27V-65, 2018-04-16, paskelbta TAR 2018-04-17, i. k. 2018-06160
Dėl Valstybės tarnybos departamento direktoriaus 2015 m. gruodžio 30 d. įsakymo Nr. 27V-157 „Dėl Valstybės tarnautojų registro ir Valstybės tarnybos valdymo informacinės sistemos duomenų saugos nuostatų patvirtinimo“ pakeitimo