Suvestinė redakcija nuo 2018-02-23 iki 2018-11-13

Įsakymas paskelbtas: TAR 2017-12-22, i. k. 2017-21049

LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTRAS

ĮSAKYMAS DĖL KAI KURIŲ LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS VALDOMŲ REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2017 m. gruodžio 22 d. Nr. 1V-883
Vilnius

Vadovaudamasis Lietuvos Respublikos kibernetinio saugumo įstatymo 13 straipsnio 5 dalimi, 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, 19 ir 26 punktais, 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:

1. T v i r t i n u Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų duomenų saugos nuostatus (pridedama).

2. P a v e d u:

2.1. Informatikos ir ryšių departamentui prie Lietuvos Respublikos vidaus reikalų ministerijos per vieną mėnesį nuo Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų duomenų saugos nuostatų (toliau – Saugos nuostatai) patvirtinimo paskirti Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų (toliau – informacinės sistemos) pagrindinį saugos įgaliotinį, pagrindinį administratorių, naudotojų administratorių ir informacinių sistemų komponentų administratorius;

2.2. informacinių sistemų tvarkytojams per vieną mėnesį nuo Saugos nuostatų patvirtinimo paskirti savo tvarkomų informacinių sistemų saugos įgaliotinius;

2.3. pagrindiniam saugos įgaliotiniui per tris mėnesius nuo Saugos nuostatų patvirtinimo parengti ir pateikti vidaus reikalų ministrui tvirtinti informacinių sistemų saugos politiką įgyvendinančių dokumentų projektus.

3. S k i r i u Informatikos ir ryšių departamentą prie Lietuvos Respublikos vidaus reikalų ministerijos atsakingu už informacinių sistemų kibernetinio saugumo organizavimą ir užtikrinimą.

4. P r i p a ž į s t u netekusiu galios Lietuvos Respublikos vidaus reikalų ministro 2007 m. sausio 2 d. įsakymo Nr. 1V-1 „Dėl Vidaus reikalų informacinės sistemos nuostatų ir Vidaus reikalų informacinės sistemos duomenų saugos nuostatų patvirtinimo“ 1.2 papunktį (su visais Vidaus reikalų informacinės sistemos duomenų saugos nuostatų pakeitimais ir papildymais).

Vidaus reikalų ministras Eimutis Misiūnas

SUDERINTA

Kibernetinio saugumo ir telekomunikacijų tarnybos
prie Krašto apsaugos ministerijos
2017 m. lapkričio 21 d. raštu Nr. IS-1037

PATVIRTINTA
Lietuvos Respublikos vidaus reikalų
ministro 2017 m. gruodžio 22 d.
įsakymu Nr. 1V-883

KAI KURIŲ LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS VALDOMŲ REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Vidaus reikalų ministerija) valdomų bei Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Informatikos ir ryšių departamentas) tvarkomų valstybės informacinių sistemų ir registrų (toliau – informacinės sistemos) elektroninės informacijos saugos politiką ir kibernetinio saugumo politiką (toliau – elektroninės informacijos saugos politika).

2. Saugos nuostatų reikalavimai taikomi tvarkant informacines sistemas, nurodytas Vidaus reikalų ministerijos valdomų ir Informatikos ir ryšių departamento tvarkomų registrų ir valstybės informacinių sistemų sąraše (Saugos nuostatų priedas).

3. Elektroninės informacijos saugos politika įgyvendinama pagal vidaus reikalų ministro tvirtinamus Vidaus reikalų ministerijos valdomų registrų ir informacinių sistemų saugos politiką įgyvendinančius dokumentus: saugaus elektroninės informacijos tvarkymo taisykles, naudotojų administravimo taisykles, veiklos tęstinumo valdymo planą (toliau – saugos politiką įgyvendinantys dokumentai).

4. Saugos nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo 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 – Bendrųjų saugos reikalavimų aprašas), Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, apraše, patvirtintame 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), vartojamas sąvokas.

5. Informacinių sistemų elektroninės informacijos sauga – tai elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas.

6. Informacinių sistemų elektroninės informacijos saugos ir kibernetinio saugumo (toliau – elektroninės informacijos sauga) užtikrinimo tikslai:

6.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti elektroninę informaciją;

6.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, praradimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

6.3. vykdyti elektroninės informacijos saugos ir kibernetinių incidentų (toliau – saugos incidentai) prevenciją.

7. Informacinių sistemų elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

7.1. elektroninės informacijos tvarkymo bei jos naudojimo kontrolė;

7.2. elektroninės informacijos tvarkymui naudojamos techninės ir programinės įrangos kontrolė;

7.3. informacinėse sistemose tvarkomų asmens duomenų apsauga;

7.4. informacinių sistemų veikos tęstinumo užtikrinimas.

8. Informacinių sistemų elektroninės informacijos saugai užtikrinti kompleksiškai naudojamos organizacinės, techninės ir programinės priemonės.

9. Saugos nuostatų reikalavimai taikomi:

9.1. informacinių sistemų valdytojai – Vidaus reikalų ministerijai, Šventaragio g. 2, Vilnius;

9.2. informacinių sistemų tvarkytojui – Informatikos ir ryšių departamentui, Šventaragio g. 2, Vilnius;

9.3. kitiems informacinių sistemų tvarkytojams, nurodytiems informacinių sistemų nuostatuose;

9.4. Informatikos ir ryšių departamento paskirtam pagrindiniam saugos įgaliotiniui;

9.5. kitų informacinių sistemų tvarkytojų paskirtiems saugos įgaliotiniams;

9.6. Informatikos ir ryšių departamento paskirtiems administratoriams;

9.7. informacinių sistemų naudotojams;

9.8. paslaugų, susijusių su informacinėmis sistemomis, teikėjams.

10. Už elektroninės informacijos saugą pagal kompetenciją atsako informacinių sistemų valdytoja ir tvarkytojai.

11. Informacinių sistemų valdytoja atsako už informacinių sistemų elektroninės informacijos saugos politikos formavimą, jos įgyvendinimo organizavimą ir priežiūrą, elektroninės informacijos ir duomenų tvarkymo bei duomenų teikimo duomenų gavėjams teisėtumą.

12. Informacinių sistemų naudotojai, tvarkantys duomenis, informaciją, dokumentus ir (arba) jų kopijas, privalo įsipareigoti saugoti duomenų ir informacijos paslaptį. Įsipareigojimas saugoti duomenų ir informacijos paslaptį galioja ir nutraukus su duomenų, informacijos, dokumentų ir (arba) jų kopijų tvarkymu susijusią veiklą.

13. Paslaugų, susijusių su informacinėmis sistemomis, teikėjai privalo įsipareigoti saugoti duomenų ir informacijos paslaptį bei pasirašyti konfidencialumo pasižadėjimą. Įsipareigojimas saugoti duomenų ir informacijos paslaptį galioja ir pasibaigus paslaugų teikimo laikui ar nutraukus šią veiklą.

14. Informacinių sistemų valdytoja atlieka informacinių sistemų nuostatuose nustatytas funkcijas, o taip pat:

14.1. tvirtina Saugos nuostatus, saugos politiką įgyvendinančius dokumentus, kitus dokumentus, susijusius su elektroninės informacijos sauga;

14.2. prižiūri ir kontroliuoja, kad informacinės sistemos būtų tvarkomos vadovaujantis informacinių sistemų nuostatais, Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais;

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

14.4. tvirtina informacinių sistemų rizikos įvertinimo ir rizikos valdymo priemonių planą ir informacinių technologijų saugos atitikties vertinimo metu nustatytų trūkumų šalinimo planą; esant poreikiui šie planai gali būti sujungti ir tvirtinamas bendras planas;

14.5. koordinuoja informacinių sistemų tvarkytojų darbą įgyvendinant elektroninės informacijos saugos reikalavimus;

14.6. nagrinėja informacinių sistemų tvarkytojų pasiūlymus dėl informacinių sistemų elektroninės informacijos saugos priemonių tobulinimo ir priima dėl jų sprendimus;

14.7. priima sprendimus dėl informacinių sistemų elektroninės informacijos saugos priemonių finansavimo;

14.8. atlieka kitas Valstybės informacinių išteklių valdymo įstatyme, Kibernetinio saugumo įstatyme, Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, informacinių sistemų nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

15. Informacinių sistemų tvarkytojas – Informatikos ir ryšių departamentas atlieka informacinių sistemų nuostatuose nustatytas funkcijas, o taip pat:

15.1. užtikrina elektroninės informacijos, esančios informacinių sistemų duomenų bazėse, saugą;

15.2. užtikrina saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais;

15.3. užtikrina tinkamą Saugos nuostatų, informacinių sistemų saugos politiką įgyvendinančių dokumentų, kitų dokumentų, susijusių su elektroninės informacijos sauga, įgyvendinimą;

15.4. rengia informacinių sistemų rizikos įvertinimo ir rizikos valdymo priemonių planą ir informacinių technologijų saugos atitikties vertinimo metu nustatytų trūkumų šalinimo planą; esant poreikiui šie planai gali būti sujungti ir rengiamas bendras planas;

15.5. planuoja ir įgyvendina priemones, mažinančias duomenų atskleidimo ir praradimo riziką bei užtikrinančias prarastų duomenų atkūrimą ir duomenų apsaugą nuo klastojimo;

15.6. užtikrina, kad informacinės sistemos veiktų nepertraukiamai;

15.7. skiria pagrindinį saugos įgaliotinį ir pagrindinį administratorių, naudotojų administratorių, informacinių sistemų komponentų administratorius;

15.8. esant informacinių sistemų tvarkytojų prašymams suteikia teisę informacinių sistemų tvarkytojams registruoti savo bei tvarkytojo įstaigai pavaldžių įstaigų informacinių sistemų naudotojus bei suteikti jiems prieigos teises;

15.9. vykdo kibernetinio saugumo organizavimo ir užtikrinimo funkcijas, nustatytas Kibernetinio saugumo įstatyme, Kibernetinio saugumo reikalavimų apraše ir kituose kibernetinį saugumą reglamentuojančiuose teisės aktuose;

15.10. vykdo Informacinių technologijų ir telekomunikacijų pagalbos tarnybos (toliau – ITT pagalbos tarnyba) funkcijas, registruoja ir valdo saugos incidentus;

15.11. atlieka kitas Valstybės informacinių išteklių valdymo įstatyme, Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, informacinių sistemų nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

16. Kiti informacinių sistemų tvarkytojai atlieka šias funkcijas:

16.1. užtikrina tinkamą informacinių sistemų valdytojos priimtų teisės aktų ir rekomendacijų, susijusių su elektroninės informacijos sauga, įgyvendinimą;

16.2. užtikrina tvarkytojo įstaigos informacinių sistemų naudotojų darbo vietose naudojamų administracinių, techninių ir programinių priemonių, užtikrinančių elektroninės informacijos saugą, diegimo koordinavimą ir priežiūrą;

16.3. pagal kompetenciją valdo informacinių sistemų kompiuterinių darbo vietų saugos incidentus, informuoja apie juos ITT pagalbos tarnybą, pagrindinį saugos įgaliotinį ir kitas atsakingas institucijas, šalina šiuos incidentus;

16.4. Informatikos ir ryšių departamentui suteikus teisę, registruoja informacinių sistemų naudotojus tvarkytojo ir jam pavaldžiose įstaigose ir suteikia šiems naudotojams prieigos teises;

16.5. paskiria savo tvarkomoms informacinėms sistemoms saugos įgaliotinį (įgaliotinius); jei informacinių sistemų tvarkytojas turi pavaldžių ar jo reguliavimo sričiai arba veiklos sričiai priskirtų kitų įstaigų (teritorinių, specializuotų, atskaitingų ir kitų) informacinių sistemų tvarkytojų (toliau – reguliavimo sričiai priskirti tvarkytojai), jis gali paskirti vieną saugos įgaliotinį, prižiūrintį ir kontroliuojantį saugos politikos įgyvendinimą savo įstaigoje ir jo reguliavimo sričiai priskirtų informacinių sistemų tvarkytojų įstaigose;

16.6. teikia pasiūlymus informacinių sistemų valdytojai dėl informacinių sistemų saugos tobulinimo;

16.7. atlieka kitas Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, informacinių sistemų nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

17. Informacinių sistemų tvarkytojai užtikrina tvarkytojo įstaigoje tvarkomos elektroninės informacijos saugą. Informacinių sistemų tvarkytojų vadovai atsako už reikiamų organizacinių ir techninių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir informacinių sistemų saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka.

18. Pagrindinis saugos įgaliotinis:

18.1. koordinuoja kitų informacinių sistemų tvarkytojų paskirtų saugos įgaliotinių veiklą;

18.2. supažindina kitų informacinių sistemų tvarkytojų paskirtus saugos įgaliotinius su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais, kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, atsakomybe už saugos dokumentų nuostatų pažeidimus;

18.3. rengia saugos dokumentų projektus;

18.4. koordinuoja ir prižiūri informacinių sistemų elektroninės informacijos saugos politikos įgyvendinimą;

18.5. koordinuoja informacinių sistemų saugos incidentų tyrimą;

18.6. teikia pasiūlymus Informatikos ir ryšių departamento direktoriui dėl:

18.6.1. informacinių sistemų informacinių technologijų saugos atitikties vertinimo atlikimo;

18.6.2. pagrindinio administratoriaus, naudotojų administratoriaus, informacinių sistemų komponentų administratorių paskyrimo;

18.7. teikia pasiūlymus informacinių sistemų valdytojai dėl Saugos nuostatų ir saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

18.8. teikia saugos įgaliotiniams ir administratoriams, prireikus ir kitiems informacinių sistemų valdytojo ir tvarkytojų darbuotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos politikos įgyvendinimu;

18.9. ne rečiau kaip kartą per kalendorinius metus organizuoja kitų informacinių sistemų tvarkytojų paskirtų saugos įgaliotinių, Informatikos ir ryšių departamento paskirtų administratorių, naudotojų saugos mokymus (surengdamas saugos tematikos mokymus, pateikdamas mokymų medžiagą Informatikos ir ryšių departamento interneto svetainėje arba organizuodamas mokymo paslaugų įsigijimą ar kitais būdais), reguliariai įvairiais būdais informuoja naudotojus apie elektroninės informacijos saugos problemas, teikia konsultacijas ir rekomendacijas (elektroniniu paštu, telefonu ir pan.).

18.10. atlieka kitas Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, informacinių sistemų nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

19. Kitų informacinių sistemų tvarkytojų paskirti saugos įgaliotiniai:

19.1. koordinuoja ir prižiūri saugos politikos įgyvendinimą informacinėse sistemose, kurioms jie paskirti, tvarkytojo įstaigoje, taip pat tvarkytojo įstaigos reguliavimo sričiai priskirtose kitose įstaigose, jei tai pavesta jų kompetencijai;

19.2. supažindina su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ir atsakomybe už juose nustatytų reikalavimų nesilaikymą tvarkytojo įstaigos naudotojus, taip pat tvarkytojo įstaigos reguliavimo sričiai priskirtų kitų įstaigų naudotojus, jei tai pavesta jų kompetencijai;

19.3. kasmet organizuoja saugos mokymus, reguliariai primena saugos problemas, teikia konsultacijas ir rekomendacijas (elektroniniu paštu, telefonu ir kt. būdais), prireikus rengia atmintines tvarkytojo įstaigos naudotojams, taip pat tvarkytojo įstaigos reguliavimo sričiai priskirtų kitų įstaigų naudotojams, jei tai pavesta jų kompetencijai;

19.4. teikia tvarkytojo įstaigos naudotojams, prireikus ir kitiems darbuotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su informacinių sistemų saugos politikos įgyvendinimu;

19.5. teikia pagrindiniam saugos įgaliotiniui siūlymus dėl Saugos nuostatų ir saugos politiką įgyvendinančių dokumentų priėmimo ir keitimo;

19.6. pagal kompetenciją dalyvauja atliekant informacinių sistemų informacinių technologijų atitikties saugos reikalavimams vertinimą bei informacinių sistemų rizikos vertinimą;

19.7. informuoja pagrindinį saugos įgaliotinį ir ITT pagalbos tarnybą apie saugos incidentus informacinėse sistemose, kurioms jie paskirti;

19.8. dalyvauja tiriant saugos incidentus;

19.9. atlieka kitas Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, informacinių sistemų nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

20. Pagrindinis saugos įgaliotinis ir kitų informacinių sistemų tvarkytojų paskirti saugos įgaliotiniai negali atlikti administratorių funkcijų.

21. Informatikos ir ryšių departamento paskirti administratoriai atlieka funkcijas, susijusias su informacinių sistemų naudotojų teisių valdymu, informacinės sistemos komponentais (kompiuteriais, operacinėmis sistemomis, duomenų bazių valdymo sistemomis, taikomųjų programų sistemomis, ugniasienėmis, įsilaužimų aptikimo sistemomis, elektroninės informacijos perdavimu tinklais, bylų serveriais ir kitais), šių informacinių sistemų komponentų sąranka, informacinių sistemų pažeidžiamų vietų nustatymu, saugumo reikalavimų atitikties nustatymu ir stebėsena, reagavimu į elektroninės informacijos saugos incidentus ir jų valdymu, taip pat privalo vykdyti visus saugos įgaliotinio nurodymus ir pavedimus, susijusius su informacinės sistemos saugos užtikrinimu, ir nuolat teikti saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę.

22. Informatikos ir ryšių departamento skiriami administratoriai:

22.1. pagrindinis administratorius, kuris prižiūri ir koordinuoja kitų Informatikos ir ryšių departamento paskirtų administratorių veiklą, prižiūri informacinių sistemų infrastruktūrą, užtikrina jos veikimą ir informacinių sistemų elektroninės informacijos saugą;

22.2. naudotojų administratorius, kuris atlieka informacinių sistemų naudotojų teisių valdymo funkcijas (informacinių sistemų naudotojų duomenų administravimas, klasifikatorių tvarkymas, registracijos žurnalų įrašų analizė ir kt.);

22.3. informacinių sistemų komponentų administratoriai, kurie atlieka funkcijas, susijusias su informacinių sistemų komponentais, šių informacinių sistemų komponentų sąranka:

22.3.1. kompiuterių tinklų administratorius atlieka šias funkcijas:

22.3.1.1. užtikrina kompiuterių tinklų veikimą;

22.3.1.2. projektuoja kompiuterių tinklus;

22.3.1.3. diegia, konfigūruoja ir prižiūri kompiuterių tinklų aktyviąją įrangą;

22.3.1.4. administruoja ugniasienes;

22.3.1.5. administruoja maršrutizatorius ir komutatorius;

22.3.1.6. administruoja pagalbinę įrangą (UPS, fizines linijas ir pan.);

22.3.1.7. užtikrina kompiuterių tinklų saugumą (nustato pažeidžiamas vietas);

22.3.2. tarnybinių stočių administratorius atlieka šias funkcijas:

22.3.2.1. užtikrina tarnybinių stočių veikimą;

22.3.2.2. konfigūruoja tarnybinių stočių tinklo prieigą;

22.3.2.3. kuria ir administruoja tarnybinių stočių naudotojų registracijos į tarnybines stotis duomenis;

22.3.2.4. stebi ir analizuoja tarnybinių stočių veiklą;

22.3.2.5. diegia ir konfigūruoja tarnybinių stočių programinę įrangą;

22.3.2.6. diegia tarnybinių stočių programinės įrangos atnaujinimus, laikydamasis informacinių sistemų pokyčių tvarkos, nustatytos informacinių sistemų valdytojos tvirtinamame informacinių sistemų pokyčių tvarkos apraše;

22.3.2.7. užtikrina tarnybinių stočių saugą;

22.3.3. duomenų bazių administratorius atlieka šias funkcijas:

22.3.3.1. užtikrina duomenų bazių veikimą;

22.3.3.2. tvarko duomenų bazių programinę įrangą;

22.3.3.3. diegia duomenų bazių programinės įrangos atnaujinimus, laikydamasis informacinių sistemų pokyčių tvarkos, nustatytos informacinių sistemų valdytojos tvirtinamame informacinių sistemų pokyčių tvarkos apraše;

22.3.3.4. kuria ir administruoja duomenų bazių naudotojų registracijos į duomenų bazes duomenis;

22.3.3.5. kuria ir atkuria atsargines elektroninės informacijos kopijas;

22.3.3.6. stebi duomenų bazes ir optimizuoja jų funkcionavimą;

22.3.3.7. užtikrina duomenų bazių saugą;

22.3.4. kitų informacinių sistemų komponentų administratoriai atlieka funkcijas, susijusias su kitų komponentų sąranka, veikimo stebėsena ir analize, profilaktine priežiūra, programinės įrangos diegimu ir konfigūravimu, trikdžių diagnostika ir šalinimu, nepertraukiamo informacinių sistemų veikimo užtikrinimu, pasiūlymų dėl jų veikimo optimizavimo teikimu.

23. Informatikos ir ryšių departamento paskirti administratoriai:

23.1. pagal kompetenciją reaguoja į saugos incidentus ir juos valdo, atlieka įsilaužimų į informacines sistemas aptikimo funkcijas;

23.2. dalyvauja atliekant informacinių sistemų rizikos vertinimą ir informacinių sistemų informacinių technologijų atitikties saugos reikalavimas vertinimą.

24. Informatikos ir ryšių departamento paskirti administratoriai yra atsakingi už tinkamą informacinių sistemų saugos dokumentuose nustatytų funkcijų vykdymą.

25. Informatikos ir ryšių departamento paskirti administratoriai privalo vykdyti visus pagrindinio saugos įgaliotinio nurodymus ir pavedimus dėl informacinių sistemų elektroninės informacijos saugos užtikrinimo, pagal kompetenciją reaguoti į saugos incidentus, juos valdyti, ir nuolat teikti pagrindiniam saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę.

26. Teisės aktai, kuriais vadovaujantis tvarkoma informacinių sistemų elektroninė informacija ir užtikrinama jos sauga:

26.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

26.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

26.3. Lietuvos Respublikos kibernetinio saugumo įstatymas;

26.4. Bendrųjų saugos reikalavimų aprašas;

26.5. Kibernetinio saugumo reikalavimų aprašas;

26.6. 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 reikalavimai);

26.7. 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 asmens duomenų saugumo priemonėms);

26.8. Informacinių sistemų valdytojos patvirtintas kibernetinių incidentų valdymo ypatingos svarbos informacinėje infrastruktūroje planas;

26.9. Informacinių sistemų nuostatai;

26.10. Lietuvos standartai LST EN ISO/IEC 27002 ir LST EN ISO/IEC 27001 bei Lietuvos ir tarptautiniai „Informacijos technologijos. Saugumo metodai“ grupės standartai, reglamentuojantys saugų duomenų tvarkymą;

26.11. kiti teisės aktai, reglamentuojantys elektroninės informacijos tvarkymo teisėtumą ir elektroninės informacijos saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

27. Informacinėse sistemose tvarkomos elektroninės informacijos svarbos kategorija, informacinių sistemų kategorijos bei priskyrimo tam tikrai kategorijai kriterijai nurodyti Saugos nuostatų priede.

28. Informacinių sistemų asmens duomenų tvarkymas automatiniu būdu priskiriamas trečiajam saugumo lygiui, vadovaujantis Bendrųjų reikalavimų asmens duomenų saugumo priemonėms 11.3 papunkčio nuostatomis.

29. Informacinių sistemų saugos priemonės parenkamos įvertinus galimus rizikos veiksnius elektroninės informacijos vientisumui, konfidencialumui ir prieinamumui.

30. Pagrindinės informacinių sistemų rizikos mažinimo priemonės išdėstomos rizikos įvertinimo ataskaitoje, kurią kasmet ne vėliau nei iki spalio 1 dienos, o prireikus ir neeilinio rizikos įvertinimo ataskaitą iki informacinių sistemų valdytojos nurodytos datos rengia pagrindinis saugos įgaliotinis, įvertinęs galinčius turėti įtakos elektroninės informacijos saugai rizikos veiksnius, iš kurių svarbiausieji yra šie:

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

30.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugos pažeidimai, vagystės ir kita);

30.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 84 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

31. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano duomenis bei jų kopijas informacinės sistemos valdytoja ar jos įgaliotas informacinės sistemos tvarkytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų patvirtinimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai (toliau – ARSIS) 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“, nustatyta tvarka.

32. Informacinių sistemų rizikos veiksnių vertinimui naudojama ARSIS.

33. Elektroninės informacijos saugos būklė gerinama techninėmis, programinėmis, organizacinėmis ir kitomis informacinių sistemų elektroninės informacijos saugos priemonėmis, kurios pasirenkamos atsižvelgiant į informacinių sistemų valdytojos skiriamus išteklius, vadovaujantis šiais principais:

33.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

33.2. elektroninės informacijos saugos priemonės diegimo kainos turi atitikti saugomos elektroninės informacijos vertę;

33.3. esant galimybei, turi būti įdiegtos prevencinės korekcinės elektroninės informacijos saugos priemonės.

34. Informacinių sistemų valdytoja, atsižvelgdama į informacinių sistemų rizikos įvertinimo ataskaitą, prireikus tvirtina patvirtinti Informatikos ir ryšių departamento parengtą rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

35. Siekiant užtikrinti Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, Informacinių technologijų saugos atitikties vertinimo metodikoje, patvirtintoje Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“, nustatyta tvarka, kasmet organizuojamas informacinių sistemų informacinių technologijų saugos reikalavimų atitikties vertinimas.

36. Informacinių sistemų informacinių technologijų saugos atitikties vertinimo metu gali būti atliekamas pažeidžiamumų testavimas imituojant kibernetines atakas bei vykdant kibernetinių incidentų imitavimo pratybas. Imituojant kibernetines atakas rekomenduojama vadovautis tarptautiniu mastu pripažintų organizacijų (pvz., EC-COUNCIL, ISACA, NIST ir kt.) rekomendacijomis ir gerąja praktika.

37. Atlikus informacinių sistemų informacinių technologijų saugos reikalavimų atitikties vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato informacinių sistemų valdytoja.

38. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano duomenis ir jų kopijas informacinių sistemų valdytoja arba jos įgaliotas tvarkytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia ARSIS 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“, nustatyta tvarka.

39. Ne rečiau kaip kartą per trejus metus informacinių sistemų informacinių technologijų saugos reikalavimų atitikties vertinimą turi atlikti nepriklausomi, visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų auditoriai.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

40. Programinės įrangos, skirtos informacines sistemas apsaugoti nuo kenksmingosios programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos ir jos atnaujinimo reikalavimai:

40.1. Informacinių sistemų tarnybinėse stotyse ir kompiuterizuotose darbo vietose turi būti naudojamos centralizuotai valdomos kenksmingosios programinės įrangos aptikimo priemonės, nuolat ieškančios ir blokuojančios kenksmingąją programinę įrangą, kurios turi būti reguliariai atnaujinamos automatiniu būdu ne rečiau kaip kartą per 24 valandas;

40.2. Programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

41. Programinės įrangos, įdiegtos informacinių sistemų tarnybinėse stotyse ir kompiuterizuotose darbo vietose, naudojimo nuostatos:

41.1. informacinių sistemų darbui turi būti naudojama tik legali ir patikrinta programinė įranga, įtraukta į leistinos programinės įrangos sąrašą, patvirtintą IRD. Leistinos programinės įrangos sąrašą turi parengti ir pagal poreikį peržiūrėti bei prireikus atnaujinti pagrindinis saugos įgaliotinis kartu su pagrindiniu administratoriumi;

41.2. programinė įranga atnaujinama laikantis gamintojo reikalavimų;

41.3. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka administratoriai;

42. Informacinėse sistemose turi būti naudojamos tik tarnybinės išorinės duomenų laikmenos (USB, CD/DVD ir kt.) bei kiti tarnybiniai įrenginiai, kurie yra išduoti tarnybinėms funkcijoms vykdyti.

43. Informacinių sistemų kompiuterizuotose darbo vietose turi būti įdiegtos priemonės, leidžiančios riboti išorinių duomenų laikmenų (USB, CD/DVD ir kt.) naudojimą.

44. Informacinių sistemų programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims.

45. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kt.) pagrindinės naudojimo nuostatos:

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

45.2. visas duomenų srautas į internetą ir iš jo turi būti filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingosios programinės įrangos;

45.3. turi būti naudojamos turinio filtravimo sistemos.

46. Informacinėse sistemose naudojamų interneto svetainių (toliau – svetainės) saugos valdymo reikalavimai:

46.1. svetainės turi atitikti Kibernetinio saugumo reikalavimų apraše ir Techniniuose reikalavimuose nustatytus reikalavimus;

46.2. svetainių užkardos turi būti sukonfigūruotos taip, kad prie svetainių turinio valdymo sistemų (toliau – TVS) būtų galima jungtis tik iš vidinio informacinių sistemų tvarkytojo kompiuterinio tinklo arba nustatytų IP (angl. *Internet Protocol*) adresų;

46.3. turi būti pakeistos numatytos prisijungimo prie svetainių turinio valdymo sistemos (TVS) ir administravimo skydų (angl. *Panel*) nuorodos (angl. *Default path*) ir slaptažodžiai;

46.4. turi būti užtikrinama, kad prie svetainių TVS ir administravimo skydų būtų galima jungtis tik naudojantis šifruotu ryšiu;

46.5. informacinėse sistemose naudojamų svetainių sauga turi būti vertinama informacinių sistemų rizikos įvertinimo metu ir (arba) informacinių sistemų informacinių technologijų saugos atitikties vertinimo metu, atliekamų Saugos nuostatų II skyriuje nustatyta tvarka.

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

47.1. informacinių sistemų naudotojų, jų vykdytų užklausų ir peržiūrėtų užklausų rezultatų duomenys tvarkomi informacinių sistemų naudotojų administravimo posistemėje Vidaus reikalų informacinės sistemos centrinio duomenų banko duomenų peržiūros kontrolės taisyklių, patvirtintų vidaus reikalų ministro 2005 m. kovo 9 d. įsakymu Nr. 1V-68 „Dėl Vidaus reikalų informacinės sistemos centrinio duomenų banko duomenų peržiūros kontrolės taisyklių patvirtinimo“, nustatyta tvarka;

47.2. tiesioginė prieiga prie informacinių sistemų elektroninės informacijos suteikiama įgyvendinus informacinių sistemų naudotojų autentifikavimo priemones – šie naudotojai savo tapatybę patvirtina slaptažodžiu ar kita autentifikavimo priemone; tiesioginė prieiga prie informacinių sistemų užtikrinama automatiniu būdu ištisą parą darbo ir poilsio dienomis.

47.3. prieiga prie informacinių sistemų suteikiama tik registruotiems informacinių sistemų naudotojams;

47.4. informacinių sistemų elektroninė informacija perduodama automatiniu būdu naudojant TCP/IP, HTTPS protokolus realiame laike (*angl. „On-line“* režimu) arba asinchroniniu režimu pagal informacinių sistemų duomenų teikimo sutartis, kuriose nustatytos perduodamos elektroninės informacijos specifikacijos, kopijų skaičius, kitos elektroninės informacijos perdavimo sąlygos ir tvarka;

47.5. informacinių sistemų elektroninė informacija, perduodama per Vidaus reikalų telekomunikacinio tinklo (toliau – VRTT) ir kitas duomenų perdavimo linijas, turi būti šifruojama.

48. Informacinių sistemų elektroninės informacijos perdavimui naudojamas VRTT ir kiti saugūs elektroninių ryšių tinklai.

49. Informacinių sistemų tvarkytojai apie diegiamus vietinius belaidžius tinklus, sujungimus su kitais tinklais, vietinių tinklų įrangos pakeitimus turi raštu informuoti Informatikos ir ryšių departamentą - VRTT pagrindinį tvarkytoją.

50. Visos informacinių sistemų naudotojų kompiuterizuotos darbo vietos turi būti valdomos naudojant centralizuoto valdymo priemones (pvz., katalogų tarnybą „*Active direktory*“).

51. Informacinių sistemų naudotojų tarnybinėms funkcijoms vykdyti naudojamuose nešiojamuose kompiuteriuose turi būti naudojamas kompiuterio įjungimo slaptažodis, papildomas informacinių sistemų naudotojo tapatybės patvirtinimas ir elektroninės informacijos šifravimas.

52. Informacinių sistemų naudotojams, kuriems atliekant tiesiogines pareigas būtina prisijungti iš nutolusios darbo vietos, gali būti suteikiama nuotolinio prisijungimo prie informacinių sistemų galimybė:

52.1. 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);

52.2. prie informacinių sistemų prisijungiama nuotoliniu būdu naudojant interneto naršyklę (HTTPS protokolą).

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

53.1. informacinių sistemų elektroninės informacijos kopijos turi būti daromos automatiškai kiekvieną dieną; prireikus jas atkurti turi teisę Informatikos ir ryšių departamento paskirtas duomenų bazių administratorius;

53.2. atkūrimas iš elektroninės informacijos kopijų privalo būti išbandomas;

53.3. informacinių sistemų elektroninės informacijos kopijos saugomos kitoje patalpoje nei informacinių sistemų tarnybinės stotys.

54. Turi būti užtikrintas saugos incidentų, įvykusių informacinėse sistemose, registravimas, valdymas ir tyrimas Kibernetinių saugumo reikalavimų aprašo bei informacinių sistemų valdytojos patvirtintų kibernetinių incidentų valdymo ypatingos svarbos informacinėje infrastruktūroje plano ir informacinių sistemų veiklos tęstinumo valdymo plano nustatyta tvarka:

54.1. registruojami informacinėse sistemose įvykę saugos incidentai ir nedelsiant į juos reaguojama, techninėmis ir programinėmis priemonėmis saugos incidentai valdomi, tiriami ir šalinami bei atkuriama sistemų veikla;

54.2. Nacionaliniam kibernetinio saugumo centrui ir kitoms atsakingoms institucijoms pagal kompetenciją pranešama apie įvykusius saugos incidentus, jų vertinimą ir suvaldymą.

55. Ne rečiau kaip kartą per savaitę turi būti atliekama informacinių sistemų naudotojų veiksmų audito įrašų analizė (esant poreikiui Informatikos ir ryšių departamentas apie informacinių sistemų naudotojų atliktus veiksmus informaciją teikia atitinkamiems informacinių sistemų tvarkytojams).

56. Ne rečiau kaip kartą per mėnesį turi būti atliekama ugniasienių užfiksuotų įvykių analizė ir pastebėtos neatitiktys saugumo reikalavimams nedelsiant šalinamos.

57. Ne rečiau kaip kartą per mėnesį turi būti įvertinami kibernetiniam saugumui užtikrinti naudojamų priemonių programiniai atnaujinimai, klaidų taisymai ir šie atnaujinimai diegiami.

58. Perkant paslaugas, darbus ar įrangą, susijusius su informacinėmis sistemomis, jų projektavimu, kūrimu, diegimu, modernizavimu, priežiūra, palaikymu, saugos užtikrinimu, auditavimu, patalpų priežiūra, elektroninės informacijos perdavimo tinklais, taip pat kitus, suteikiančius teisę ir galimybę prieiti prie elektroninės informacijos, ją apdoroti, saugoti, keistis elektronine informacija ar tiekti informacinių technologijų infrastruktūros komponentus, pirkimo dokumentuose iš anksto turi būti nustatyta, kad paslaugų teikėjas, darbų vykdytojas ar techninės ir programinės įrangos tiekėjas (toliau – paslaugų teikėjas) privalo laikytis informacinių sistemų saugos dokumentuose nustatytų reikalavimų ir užtikrinti teikiamų paslaugų, vykdomų darbų ar tiekiamos įrangos atitiktį nustatytiems elektroninės informacijos saugos reikalavimams.

59. Į paslaugų pirkimo sutartį turi būti įtraukta nuostata, įpareigojanti paslaugų teikėjo darbuotojus pasirašyti konfidencialumo pasižadėjimą neatskleisti tretiesiems asmenims jokios informacijos, gautos vykdant šią sutartį, išskyrus tiek, kiek būtina sutarties vykdymui, o taip pat nenaudoti konfidencialios informacijos asmeniniams ar trečiųjų asmenų poreikiams laikantis principo, kad visa paslaugų teikėjui suteikta informacija (įskaitant informacinėse sistemose tvarkomą elektroninę informaciją) yra konfidenciali, nebent raštu patvirtinama, kad tam tikra pateikta informacija nėra konfidenciali.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

60. Pagrindinis saugos įgaliotinis ir saugos įgaliotiniai privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis Bendrųjų saugos reikalavimų aprašu, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą, privalo tobulinti kvalifikaciją elektroninės informacijos saugos srityje.

61. Saugos įgaliotiniu, administratoriumi 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 vieneri metai.

62. Visi administratoriai privalo išmanyti pagrindinius elektroninės informacijos saugos ir saugaus darbo su duomenų perdavimo tinklais principus, atsižvelgiant į vykdomas funkcijas atitinkamai turėti sisteminių programinių priemonių administravimo ir priežiūros patirties, mokėti administruoti ir prižiūrėti duomenų bazes, gebėti užtikrinti techninės ir programinės įrangos nepertraukiamą funkcionavimą bei saugą, stebėti techninės ir programinės įrangos veikimą, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, sutrikimų bei saugos incidentų diagnostiką ir šalinimą, turėti sisteminių programinių priemonių (*Windows, Unix, Oracle*) administravimo ir priežiūros patirties.

63. Visi administratoriai ir naudotojai turi būti susipažinę su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais, pagal kompetenciją ir kitais teisės aktais bei standartais, reglamentuojančiais elektroninės informacijos saugą.

64. Naudotojai, tvarkantys elektroninę informaciją, privalo įsipareigoti saugoti informacijos paslaptį. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą bei valstybės tarnybos ar darbo santykius.

65. Naudotojai, atliekantys tarnybines funkcijas, susijusias su asmens duomenų tvarkymu bei teikimu, raštu pasirašytinai įpareigojami saugoti asmens duomenų paslaptį. Asmens duomenų paslaptį jie privalo saugoti ir pasibaigus darbo (tarnybos) santykiams, per visą asmens duomenų teisinės apsaugos laiką, jeigu Asmens duomenų teisinės apsaugos įstatymas nenumato ko kita.

66. Naudotojai, pastebėję saugos dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai Informatikos ir ryšių departamento ITT pagalbos grupei arba administratoriui ar saugos įgaliotiniui.

67. Informacinių sistemų naudotojai privalo:

67.1. turėti pagrindinių darbo kompiuteriu, taikomosiomis programomis įgūdžių, mokėti saugiai tvarkyti elektroninę informaciją;

67.2. nuolat kelti kvalifikaciją saugaus elektroninės informacijos tvarkymo kursuose, mokymuose, seminaruose;

67.3. pamiršę, praradę arba kitaip netekę savo prisijungimo prie informacinės sistemos vardo ar slaptažodžio, nedelsiant elektroniniu paštu arba telefonu informuoti naudotojų administratorių.

68. Informacinių sistemų naudotojams draudžiama:

68.1. atskleisti informacinės sistemos duomenis ar suteikti kitokią galimybę bet kokia forma su jais susipažinti tokios teisės neturintiems asmenims;

68.2. savavališkai diegti informacinės sistemos taikomosios programinės įrangos pakeitimus ir naujas versijas neturint tam suteiktos teisės;

68.3. atskleisti kitiems asmenims prisijungimo prie informacinės sistemos vardą, slaptažodį ar kitaip sudaryti sąlygas jais pasinaudoti;

68.4. naudoti informacinės sistemos duomenis kitokiais nei jų nuostatuose nurodytais tikslais bei savo pareigybės aprašyme nustatytų funkcijų vykdymo tikslais;

68.5. sudaryti sąlygas pasinaudoti informacinei sistemai tvarkyti naudojama technine ir programine įranga tokios teisės neturintiems asmenims (paliekant darbo vietą būtina užrakinti darbalaukį arba išjungti darbo stotį);

68.6. atlikti veiksmus, dėl kurių gali būti neteisėtai pakeisti, sunaikinti ar atskleisti informacinės sistemos duomenys, taip pat neatlikti būtinų veiksmų, kurie apsaugo informacinės sistemos duomenis;

68.7. atlikti bet kokius kitus neteisėtus informacinės sistemos tvarkymo veiksmus.

69. Informacinių sistemų naudotojams ne rečiau kaip kartą per kalendorinius metus turi būti rengiami elektroninės informacijos saugos mokymai, įvairiais būdais primenama apie saugos problematiką (pvz., priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės ir pan.). Saugos mokymai organizuojami periodiškai, mokymus organizuoja pagrindinis saugos įgaliotinis ir kitų informacinių sistemų tvarkytojų paskirti saugos įgaliotiniai pagal kompetenciją.

V SKYRIUS
INFORMACINIŲ SISTEMŲ NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

70. Tvarkyti informacinių sistemų elektroninę informaciją gali tik informacinių sistemų naudotojai, susipažinę su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugą, taip pat atsakomybe už saugos dokumentų nuostatų pažeidimus, ir sutikę laikytis saugos dokumentuose nustatytų reikalavimų. Pakartotinis supažindinimas yra vykdomas pasikeitus minėtiems dokumentams ir teisės aktams.

71. Informacinių sistemų naudotojų supažindinimą su Saugos nuostatais ir informacinių sistemų saugos politiką įgyvendinančiais dokumentais pagal kompetenciją organizuoja saugos įgaliotiniai.

72. Informacinių sistemų naudotojai su Saugos nuostatais ir informacinių sistemų saugos politiką įgyvendinančiais dokumentais bei atsakomybe už jų reikalavimų nesilaikymą supažindinami pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodomumą (jungiantis prie informacinės sistemos per naudotojo sąsają ar pan.).

73. Saugos nuostatai ir informacinių sistemų saugos politiką įgyvendinantys dokumentai turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per kalendorinius metus. Informacinių sistemų saugos dokumentai turi būti persvarstomi (peržiūrimi) atlikus rizikos veiksnių analizę ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams. Saugos įgaliotiniai pagal kompetenciją atsakingi, kad informacinių sistemų naudotojai būtų informuoti apie jų pakeitimą ir (ar) pripažinimą netekusiais galios.

_____

Kai kurių Vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų duomenų saugos nuostatų
priedas

VIDAUS REIKALŲ MINISTERIJOS VALDOMŲ IR INFORMATIKOS IR RYŠIŲ DEPARTAMENTO PRIE VIDAUS REIKALŲ MINISTERIJOS TVARKOMŲ REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ SĄRAŠAS

Eil. Nr.	Registro / valstybės informacinės sistemos pavadinimas	Registro / valstybės informacinės sistemos elektroninės informacijos svarbos kategorija	Registro / valstybės informacinės sistemos kategorija	Registro / valstybės informacinės sistemos priskyrimo kategorijai kriterijai
1.	Administracinių nusižengimų registras	ypatingos svarbos	1	Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo (toliau – Aprašas) 7.1, 7.2 ir 12.1 papunkčiai
2.	Užsieniečių registras	ypatingos svarbos	1	Aprašo 7.1, 7.2 ir 12.1 papunkčiai
3.	Ieškomų asmenų, neatpažintų lavonų ir nežinomų bejėgių asmenų žinybinis registras	ypatingos svarbos	1	Aprašo 7.1, 7.2 ir 12.1 papunkčiai
4.	Nusikalstamų veikų žinybinis registras	svarbi	2	Aprašo 8.1, 8.2 ir 12.2 papunkčiai
5.	Vidaus reikalų pareigūnų registras	svarbi	2	Aprašo 8.1, 8.2 ir 12.2 papunkčiai

6.	Habitoskopinių duomenų registras	svarbi	2	Aprašo 8.1, 8.2 ir 12.2 papunkčiai
7.	Integruota baudžiamojo proceso informacinė sistema	ypatingos svarbos	1	Aprašo 7.1, 7.2 ir 12.1 papunkčiai
8.	Lietuvos nacionalinė Šengeno informacinė sistema	ypatingos svarbos	1	Aprašo 7.1, 7.2 ir 12.1 papunkčiai
9.	Lietuvos nacionalinė vizų informacinė sistema	ypatingos svarbos	1	Aprašo 7.1, 7.2 ir 12.1 papunkčiai
10.	Nacionalinė elektroninės atpažinties informacinė sistema	ypatingos svarbos	1	Aprašo 7.2, 7.6 ir 12.1 papunkčiai
11.	Vidaus reikalų informacinė sistema	ypatingos svarbos	1	Aprašo 7.2, 7.6 ir 12.1 papunkčiai
12.	Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistema	svarbi	2	Aprašo 8.1, 8.2 ir 12.2 papunkčiai
13.	Sertifikatų valdymo informacinė sistema	svarbi	2	Aprašo 8.1, 8.2 ir 12.2 papunkčiai
14.	Viešųjų ir administracinių paslaugų stebėsenos ir analizės informacinė sistema	vidutinės svarbos	3	Aprašo 9.1, 9.2 ir 12.3 papunkčiai
15.	Viešojo administravimo subjektų sistemos stebėsenos (monitoringo) informacinė sistema	mažiausios svarbos	4	Aprašo 10 punktas ir 12.4 papunktis
16.	Lietuvos migracijos informacinė sistema	svarbi	2	Aprašo 8.1, 8.2 ir 12.2 papunkčiai

_____

Priedo pakeitimai:
Nr. 1V-151, 2018-02-22, paskelbta TAR 2018-02-22, i. k. 2018-02744

Pakeitimai:

1.
Lietuvos Respublikos vidaus reikalų ministerija, Įsakymas
Nr. 1V-151, 2018-02-22, paskelbta TAR 2018-02-22, i. k. 2018-02744
Dėl Lietuvos Respublikos vidaus reikalų ministro 2017 m. gruodžio 22 d. įsakymo Nr. 1V-883 „Dėl Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų duomenų saugos nuostatų patvirtinimo“ pakeitimo