Suvestinė redakcija nuo 2020-12-16 iki 2021-06-25

Įsakymas paskelbtas: TAR 2019-10-04, i. k. 2019-15863

PRIEŠGAISRINĖS APSAUGOS IR GELBĖJIMO DEPARTAMENTO PRIE VIDAUS REIKALŲ MINISTERIJOS DIREKTORIUS

ĮSAKYMAS DĖL PRIEŠGAISRINĖS APSAUGOS IR GELBĖJIMO DEPARTAMENTO PRIE VIDAUS REIKALŲ MINISTERIJOS VALDOMŲ VALSTYBĖS INFORMACINIŲ SISTEMŲ IR VALSTYBINĖS REIKŠMĖS IR PAVOJINGŲ OBJEKTŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2019 m. spalio 4 d. Nr. 1-414
Vilnius

Vadovaudamasis Lietuvos Respublikos kibernetinio saugumo įstatymo 11 straipsnio 1 dalies 5 punktu, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 44 straipsnio 2 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“, 12 ir 19 punktais:

1. T v i r t i n u Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos valdomų valstybės informacinių sistemų ir Valstybinės reikšmės ir pavojingų objektų registro duomenų saugos nuostatus (toliau – Saugos nuostatai) (pridedama).

2. S k i r i u:

2.1. Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos (toliau – departamentas) Materialinių išteklių valdymo valdybos Informacinių technologijų ir ryšių skyrių atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą;

Papunkčio pakeitimai:
Nr. 1-631, 2020-12-15, paskelbta TAR 2020-12-15, i. k. 2020-27318

2.2. departamento Materialinių išteklių valdymo valdybos Informacinių technologijų ir ryšių skyriaus informacinių technologijų ir ryšių saugumo specialistę Palmirą Ožalinskienę departamento valdomų valstybės informacinių sistemų ir Valstybinės reikšmės ir pavojingų objektų registro saugos įgaliotine.

Papunkčio pakeitimai:
Nr. 1-311, 2020-07-03, paskelbta TAR 2020-07-03, i. k. 2020-14988
Nr. 1-631, 2020-12-15, paskelbta TAR 2020-12-15, i. k. 2020-27318

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

3.1. departamento direktoriaus 2009 m. sausio 30 d. įsakymo Nr. 1-28 „Dėl Valstybinės priešgaisrinės gelbėjimo tarnybos informacinės sistemos nuostatų ir Valstybinės priešgaisrinės gelbėjimo tarnybos informacinės sistemos duomenų saugos nuostatų patvirtinimo“ 1.2 papunktį ir 2 punktą;

3.2. departamento direktoriaus 2011 m. gegužės 18 d. įsakymą Nr.1-178 „Dėl Valstybinės priešgaisrinės priežiūros veiklos administravimo informacinės sistemos duomenų saugos nuostatų patvirtinimo“;

3.3. departamento direktoriaus 2011 m. gruodžio 5 d. įsakymo Nr. 1-342 „Dėl Gyventojų perspėjimo ir informavimo informacinės sistemos nuostatų ir Gyventojų perspėjimo ir informavimo informacinės sistemos duomenų saugos nuostatų patvirtinimo“ 2 punktą;

3.4. departamento direktoriaus 2016 m. sausio 4 d. įsakymo Nr. 1/2015-412 „Dėl Valstybinės reikšmės ir pavojingų objektų registro duomenų saugos nuostatų, Valstybinės reikšmės ir pavojingų objektų registro saugaus elektroninės informacijos tvarkymo taisyklių, Valstybinės reikšmės ir pavojingų objektų registro naudotojų administravimo taisyklių ir Valstybinės reikšmės ir pavojingų objektų registro veiklos tęstinumo valdymo plano patvirtinimo“ 1.1 papunktį ir 3 punktą;

3.5. departamento direktoriaus 2016 m. sausio 27 d. įsakymą Nr. 1-24 „Dėl Gyventojų perspėjimo ir informavimo informacinės sistemos duomenų saugos nuostatų patvirtinimo“;

3.6. departamento direktoriaus 2018 m. spalio 11 d. įsakymą Nr.1-361 „Dėl Kai kurių Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos valdomų valstybės informacinių sistemų ir registro duomenų saugos nuostatų patvirtinimo“;

3.7. Specialiosios priešgaisrinės gelbėjimo valdybos direktoriaus 2018 m. lapkričio 28 d. įsakymą Nr. 4-265 „Dėl atsakingų darbuotojų paskyrimo“.

Direktoriaus pavaduotojas,
atliekantis direktoriaus funkcijas,
vidaus tarnybos pulkininkas Mindaugas Kanapickas

PATVIRTINTA
Priešgaisrinės apsaugos ir gelbėjimo
departamento prie Vidaus reikalų
ministerijos direktoriaus
2019 m. spalio 4 d. įsakymu Nr. 1-414

PRIEŠGAISRINĖS APSAUGOS IR GELBĖJIMO DEPARTAMENTO PRIE VIDAUS REIKALŲ MINISTERIJOS VALDOMŲ VALSTYBĖS INFORMACINIŲ SISTEMŲ IR VALSTYBINĖS REIKŠMĖS IR PAVOJINGŲ OBJEKTŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos valdomų valstybės informacinių sistemų ir Valstybinės reikšmės ir pavojingų objektų registro duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos (toliau – departamentas) valdomų valstybės informacinių sistemų ir Valstybinės reikšmės ir pavojingų objektų registro (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 Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos valdomų valstybės informacinių sistemų ir registro sąraše (Saugos nuostatų priedas).

3. Elektroninės informacijos saugos politika įgyvendinama vadovaujantis departamento direktoriaus tvirtintais Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos valdomų informacinių sistemų ir Valstybinės reikšmės ir pavojingų objektų registro saugos politiką įgyvendinančiais dokumentais: saugaus elektroninės informacijos tvarkymo taisyklėmis, naudotojų administravimo taisyklėmis, veiklos tęstinumo valdymo planu (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 kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. nutarimu Nr. 1209 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“ pakeitimo“ (toliau – Kibernetinio saugumo reikalavimų aprašas), vartojamas sąvokas.

5. Informacinių sistemų elektroninės informacijos (toliau – elektroninė informacija) sauga – tai elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas.

6. 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. Elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

7.1. elektroninės informacijos tvarkymo ir jos naudojimo kontrolė;

7.2. elektroninei informacijai tvarkyti naudojamos techninės ir programinės įrangos kontrolė;

7.3. informacinėse sistemose tvarkomų asmens duomenų apsauga;

7.4. informacinių sistemų veikos tęstinumo užtikrinimas.

8. Elektroninės informacijos saugai užtikrinti kompleksiškai naudojamos organizacinės, techninės ir programinės priemonės.

9. Saugos nuostatų reikalavimai taikomi:

9.1. informacinių sistemų valdytojui ir tvarkytojui – Priešgaisrinės apsaugos ir gelbėjimo departamentui prie Vidaus reikalų ministerijos, Švitrigailos g. 18, Vilnius;

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

9.3. departamento paskirtam saugos įgaliotiniui;

9.4. departamento paskirtiems administratoriams;

9.5. informacinių sistemų naudotojams;

9.6. paslaugų, susijusių su informacinėmis sistemomis, teikėjams.

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

11. Informacinių sistemų valdytojas atsako už 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 ir pasirašyti konfidencialumo pasižadėjimą. Įsipareigojimas saugoti duomenų ir informacijos paslaptį galioja ir pasibaigus paslaugų teikimo laikui ar nutraukus šią veiklą.

14. Informacinių sistemų valdytojas atlieka informacinių sistemų nuostatuose nustatytas funkcijas, 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 elektroninės informacijos saugos priemonių tobulinimo ir priima dėl jų sprendimus;

14.7. priima sprendimus dėl 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 ir saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

15. Informacinių sistemų tvarkytojas atlieka informacinių sistemų nuostatuose nustatytas funkcijas, 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, 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 ir užtikrinančias prarastų duomenų atkūrimą ir duomenų apsaugą nuo klastojimo;

15.6. užtikrina, kad informacinės sistemos veiktų nepertraukiamai;

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

15.8. esant kitų informacinių sistemų tvarkytojų prašymams, suteikia teisę kitiems informacinių sistemų tvarkytojams registruoti savo ir tvarkytojo įstaigai pavaldžių įstaigų informacinių sistemų naudotojus ir 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 ir saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

16. Kiti informacinių sistemų tvarkytojai atlieka šias funkcijas:

16.1. užtikrina tinkamą informacinių sistemų valdytojo 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, saugos įgaliotinį ir kitas atsakingas institucijas, šalina šiuos incidentus;

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

16.5. teikia pasiūlymus informacinių sistemų valdytojui dėl informacinių sistemų saugos tobulinimo;

16.6. atlieka kitas Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, informacinių sistemų nuostatuose ir 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 saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka.

18. Saugos įgaliotinis:

18.1. rengia saugos dokumentų projektus;

18.2. koordinuoja ir prižiūri elektroninės informacijos saugos politikos įgyvendinimą;

18.3. koordinuoja saugos incidentų tyrimą;

18.4. teikia pasiūlymus departamento direktoriui dėl:

18.4.1. informacinių sistemų informacinių technologijų saugos atitikties vertinimo atlikimo;

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

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

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

18.7. ne rečiau kaip kartą per kalendorinius metus organizuoja departamento paskirtų administratorių, naudotojų saugos mokymus (surengdamas saugos tematikos mokymus, pateikdamas mokymų medžiagą 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.);

18.8. atlieka kitas Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, informacinių sistemų nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas;

18.9. 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;

18.10. 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. Saugos įgaliotinis ir kitų informacinių sistemų tvarkytojų paskirti saugos įgaliotiniai negali atlikti administratorių funkcijų.

20. 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 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.

21. Departamento skiriami administratoriai:

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

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

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

21.3.1. kompiuterių tinklų administratorius atlieka šias funkcijas:

21.3.1.1. užtikrina kompiuterių tinklų veikimą;

21.3.1.2. projektuoja kompiuterių tinklus;

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

21.3.1.4. administruoja ugniasienes;

21.3.1.5. administruoja maršrutizatorius ir komutatorius;

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

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

21.3.2. tarnybinių stočių administratorius atlieka šias funkcijas:

21.3.2.1. užtikrina tarnybinių stočių veikimą;

21.3.2.2. konfigūruoja tarnybinių stočių tinklo prieigą;

21.3.2.3. kuria ir administruoja tarnybinių stočių naudotojų registravimo į tarnybines stotis duomenis;

21.3.2.4. stebi ir analizuoja tarnybinių stočių veiklą;

21.3.2.5. diegia ir konfigūruoja tarnybinių stočių programinę įrangą;

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

21.3.2.7. užtikrina tarnybinių stočių saugą;

21.3.3. duomenų bazių administratorius atlieka šias funkcijas:

21.3.3.1. užtikrina duomenų bazių veikimą;

21.3.3.2. tvarko duomenų bazių programinę įrangą;

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

21.3.3.4. kuria ir administruoja duomenų bazių naudotojų registravimo į duomenų bazes duomenis;

21.3.3.5. kuria ir atkuria atsargines elektroninės informacijos kopijas;

21.3.3.6. stebi duomenų bazes ir optimizuoja jų funkcionavimą;

21.3.3.7. užtikrina duomenų bazių saugą;

21.3.4. 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.

22. Departamento paskirti administratoriai:

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

22.2. dalyvauja atliekant informacinių sistemų rizikos vertinimą ir informacinių sistemų informacinių technologijų atitikties saugos reikalavimams vertinimą.

23. Departamento paskirti administratoriai yra atsakingi už tinkamą informacinių sistemų saugos dokumentuose nustatytų funkcijų vykdymą.

24. Departamento paskirti administratoriai privalo vykdyti visus saugos įgaliotinio nurodymus ir pavedimus dėl elektroninės informacijos saugos užtikrinimo, pagal kompetenciją reaguoti į saugos incidentus, juos valdyti ir nuolat teikti saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę.

25. Teisės aktai, kuriais vadovaujantis tvarkoma elektroninė informacija ir užtikrinama jos sauga:

25.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

25.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

25.3. Lietuvos Respublikos kibernetinio saugumo įstatymas;

25.4. Bendrųjų saugos reikalavimų aprašas;

25.5. Kibernetinio saugumo reikalavimų aprašas;

25.6. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – Techniniai reikalavimai);

Papunkčio pakeitimai:

Nr. 1-631, 2020-12-15, paskelbta TAR 2020-12-15, i. k. 2020-27318

25.7. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

25.8. Informacinių sistemų valdytojo patvirtintas kibernetinių incidentų valdymo ypatingos svarbos informacinėje infrastruktūroje planas;

25.9. Informacinių sistemų nuostatai;

25.10. 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;

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

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

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

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

28. 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 valdytojo nurodytos datos rengia saugos įgaliotinis, įvertinęs galinčius turėti įtakos elektroninės informacijos saugai rizikos veiksnius, iš kurių svarbiausieji yra šie:

28.1. 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);

28.2. 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);

28.3. 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.

29. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano duomenis ir jų kopijas informacinės sistemos valdytojas ar jo 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 krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

Punkto pakeitimai:

Nr. 1-631, 2020-12-15, paskelbta TAR 2020-12-15, i. k. 2020-27318

30. Informacinių sistemų rizikos veiksniams vertinti naudojama ARSIS.

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

31.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

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

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

32. Informacinių sistemų valdytojas, atsižvelgdamas į informacinių sistemų rizikos įvertinimo ataskaitą, prireikus tvirtina departamento parengtą rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

33. Siekiant užtikrinti Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, Informacinių technologijų saugos atitikties vertinimo metodikoje, patvirtintoje Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“, nustatyta tvarka kasmet organizuojamas informacinių sistemų informacinių technologijų saugos reikalavimų atitikties vertinimas.

Punkto pakeitimai:

Nr. 1-631, 2020-12-15, paskelbta TAR 2020-12-15, i. k. 2020-27318

34. Informacinių sistemų informacinių technologijų saugos atitikties vertinimo metu gali būti atliekamas pažeidžiamumų testavimas imituojant kibernetines atakas ir 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.

35. 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 valdytojas.

36. Informacinių technologijų saugos atitikties vertinimo ataskaitas, pastebėtų trūkumų šalinimo plano duomenis ir jų kopijas informacinių sistemų valdytojas 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 krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

Punkto pakeitimai:

Nr. 1-631, 2020-12-15, paskelbta TAR 2020-12-15, i. k. 2020-27318

37. 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

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

38.1. 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;

38.2. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

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

39.1. informacinių sistemų darbui turi būti naudojama tik legali ir patikrinta programinė įranga, įtraukta į leistinos programinės įrangos sąrašą, patvirtintą informacinės sistemos valdytojo.

Leistinos programinės įrangos sąrašą turi parengti ir pagal poreikį peržiūrėti bei prireikus atnaujinti saugos įgaliotinis kartu su pagrindiniu administratoriumi;

39.2. programinė įranga atnaujinama laikantis gamintojo reikalavimų;

39.3. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka administratoriai.

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

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

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

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

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

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

43.3. turi būti naudojamos turinio filtravimo sistemos.

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

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

44.2. 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;

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

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

44.5. 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.

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

45.1. 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;

45.2. 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;

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

45.4. informacinių sistemų elektroninė informacija perduodama automatiniu būdu naudojant TCP/IP, HTTPS protokolus realiuoju laiku prijungties režimu (angl. *online)* arba asinchroniniu režimu pagal informacinių sistemų duomenų teikimo sutartis, kuriose nustatytos perduodamos elektroninės informacijos specifikacijos, kopijų skaičius, kitos elektroninės informacijos perdavimo sąlygos ir tvarka;

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

46. Informacinių sistemų elektroninei informacijai perduoti naudojamas VRTT ir kiti saugūs elektroninių ryšių tinklai.

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

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

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

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

50.1. 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*);

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

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

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

51.2. atkūrimas iš elektroninės informacijos kopijų privalo būti išbandomas;

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

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

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

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

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

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

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

56. 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.

57. 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 sutarčiai vykdyti, 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

58. Saugos įgaliotinis 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.

59. 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 vieni metai.

60. 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.

61. 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.

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

63. Naudotojai, atliekantys tarnybines funkcijas, susijusias su asmens duomenų tvarkymu ir teikimu, 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.

64. Naudotojai, pastebėję saugos dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai ITT pagalbos tarnybai arba administratoriui ar saugos įgaliotiniui.

65. Informacinių sistemų naudotojai privalo:

65.1. turėti pagrindinius darbo kompiuteriu, taikomosiomis programomis įgūdžius, mokėti saugiai tvarkyti elektroninę informaciją;

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

65.3. pamiršę, praradę arba kitaip netekę savo prisijungimo prie informacinės sistemos vardą ar slaptažodį, nedelsdami elektroniniu paštu arba telefonu informuoti naudotojų administratorių.

66. Informacinių sistemų naudotojams draudžiama:

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

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

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

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

66.5. 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);

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

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

67. 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

68. 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.

69. Informacinių sistemų naudotojų supažindinimą su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais pagal kompetenciją organizuoja saugos įgaliotinis.

70. Informacinių sistemų naudotojai su Saugos nuostatais ir 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.).

71. Saugos nuostatai ir 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.

_____

Priešgaisrinės apsaugos ir gelbėjimo departamento
prie Vidaus reikalų ministerijos valdomų valstybės
informacinių sistemų ir Valstybinės reikšmės ir pavojingų
objektų registro duomenų saugos nuostatų
priedas

PRIEŠGAISRINĖS APSAUGOS IR GELBĖJIMO DEPARTAMENTO PRIE VIDAUS REIKALŲ MINISTERIJOS VALDOMŲ VALSTYBĖS INFORMACINIŲ SISTEMŲ IR REGISTRO 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.	Valstybinės reikšmės ir pavojingų objektų registras	svarbi	2	Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo (toliau – Aprašas) 8.1–8.2 ir 12.2 papunkčiai
2.	Gyventojų perspėjimo ir informavimo informacinė sistema	vidutinės svarbos	3	Aprašo 9.1–9.2 ir 12.3 papunkčiai
3.	Valstybinės priešgaisrinės priežiūros veiklos administravimo informacinė sistema	svarbi	2	Aprašo 8.1–8.2 ir 12.2 papunkčiai
4.	Valstybinės priešgaisrinės gelbėjimo tarnybos informacinė sistema	vidutinės svarbos	3	Aprašo 9.1–9.2 ir 12.3 papunkčiai

_____

Pakeitimai:

1.
Priešgaisrinės apsaugos ir gelbėjimo departamentas prie Vidaus reikalų ministerijos, Įsakymas
Nr. 1-311, 2020-07-03, paskelbta TAR 2020-07-03, i. k. 2020-14988
Dėl Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus 2019 m. spalio 4 d. įsakymo Nr. 1-414 „Dėl Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos valdomų valstybės informacinių sistemų ir Valstybinės reikšmės ir pavojingų objektų registro duomenų saugos nuostatų patvirtinimo" pakeitimo

2.
Priešgaisrinės apsaugos ir gelbėjimo departamentas prie Vidaus reikalų ministerijos, Įsakymas
Nr. 1-631, 2020-12-15, paskelbta TAR 2020-12-15, i. k. 2020-27318
Dėl Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus 2019 m. spalio 4 d. įsakymo Nr. 1-414 „Dėl Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos valdomų valstybės informacinių sistemų ir Valstybinės reikšmės ir pavojingų objektų registro duomenų saugos nuostatų patvirtinimo“ pakeitimo