Įsakymas netenka galios 2018-11-14:
Lietuvos Respublikos vidaus reikalų ministerija, Įsakymas
Nr. 1V-837, 2018-11-13, paskelbta TAR 2018-11-13, i. k. 2018-18324
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 ir kai kurių Lietuvos Respublikos vidaus reikalų ministro įsakymų, susijusių su Vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų sauga, pripažinimo netekusiais galios

Suvestinė redakcija nuo 2017-09-09 iki 2018-11-13

Įsakymas paskelbtas: TAR 2015-10-05, i. k. 2015-14749

Nauja redakcija nuo 2017-09-09:
Nr. 1V-623, 2017-09-08, paskelbta TAR 2017-09-08, i. k. 2017-14383

LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTRAS

ĮSAKYMAS DĖL ADMINISTRACINIŲ NUSIŽENGIMŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2015 m. spalio 5 d. Nr. 1V-781

Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 7.1 papunkčiu, 11, 19 ir 26 punktais, ir atsižvelgdamasį 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“, 7 punktą:

1. T v i r t i n u Administracinių nusižengimų registro duomenų saugos nuostatus (pridedama).

2. P a v e d u:

2.1. Informatikos ir ryšių departamentui prie Lietuvos Respublikos vidaus reikalų ministerijos per mėnesį nuo Administracinių nusižengimų registro duomenų saugos nuostatų patvirtinimo paskirti Administracinių nusižengimų registro (toliau – ANR) saugos įgaliotinį ir ANR administratorių;

2.2. ANR saugos įgaliotiniui per 3 mėnesius nuo Administracinių nusižengimų registro duomenų saugos nuostatų patvirtinimo parengti ir pateikti ANR valdytojui tvirtinti ANR saugos politiką įgyvendinančių dokumentų projektus.

Vidaus reikalų ministras Saulius Skvernelis

PATVIRTINTA
Lietuvos Respublikos vidaus reikalų
ministro 2015 m. spalio 5 d. įsakymu
Nr. 1V-781
(Lietuvos Respublikos vidaus reikalų
ministro 2017 m. rugsėjo 8 d.
įsakymo Nr. 1V-623 redakcija)

ADMINISTRACINIŲ NUSIŽENGIMŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Administracinių nusižengimų registro duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato Administracinių nusižengimų registro (toliau – ANR) elektroninės informacijos saugos politiką ir kibernetinio saugumo politiką (toliau – elektroninės informacijos saugos politika), organizacines, technines, programines, teisines ir kitas priemones, užtikrinančias saugų ANR elektroninės informacijos tvarkymą.

2. Saugos nuostatuose vartojamos sąvokos apibrėžtos Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir 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).

3. ANR elektroninės informacijos saugos politika įgyvendinama pagal ANR valdytojo tvirtinamus saugos politiką įgyvendinančius dokumentus:

3.1. Administracinių nusižengimų registro saugaus elektroninės informacijos tvarkymo taisykles;

3.2. Administracinių nusižengimų registro veiklos tęstinumo valdymo planą;

3.3. Administracinių nusižengimų registro naudotojų administravimo taisykles.

4. ANR elektroninės informacijos saugos ir kibernetinio saugumo (toliau – elektroninės informacijos sauga) užtikrinimo tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti ANR elektroninę informaciją, užtikrinti ANR elektroninės informacijos konfidencialumą, prieinamumą, vientisumą ir tinkamą techninės, programinės ir ryšių įrangos funkcionavimą.

5. ANR elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

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

5.2. ANR elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

5.3. ANR tvarkomų asmens duomenų apsauga;

5.4. ANR veiklos tęstinumo užtikrinimas.

6. ANR elektroninės informacijos saugai užtikrinti kompleksiškai naudojamos organizacinės, teisinės, techninės ir programinės priemonės.

7. Saugos nuostatai taikomi ANR valdytojui, ANR tvarkytojams, ANR saugos įgaliotiniams, ANR administratoriui ir ANR naudotojams.

8. ANR valdytojas – Lietuvos Respublikos vidaus reikalų ministerija (toliau – VRM), Šventaragio g. 2, Vilnius, kuri atlieka Administracinių nusižengimų registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2016 m. gruodžio 28 d. nutarimu Nr. 1278 „Dėl Administracinių teisės pažeidimų registro reorganizavimo ir Administracinių nusižengimų registro nuostatų patvirtinimo“ (toliau – ANR nuostatai), apibrėžtas funkcijas, taip pat:

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

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

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

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

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

8.6. priima sprendimą dėl ANR informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

8.7. vykdo kitas Saugos nuostatais, ANR nuostatais, Bendrųjų saugos reikalavimų aprašu, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašu, patvirtintu 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 – Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas) ir kitais teisės aktais, reglamentuojančiais ANR elektroninės informacijos tvarkymo teisėtumą ir saugos valdymą, priskirtas funkcijas.

9. ANR tvarkytojai yra:

9.1. Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Informatikos ir ryšių departamentas);

9.2. Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos;

9.3. apskričių vyriausieji policijos komisariatai, Lietuvos kelių policijos tarnyba, Lietuvos kriminalinės policijos biuras;

9.4. Lietuvos Respublikos vyriausioji rinkimų komisija;

9.5. Lietuvos kariuomenė;

9.6. Lietuvos Respublikos Seimo kontrolierių įstaiga;

9.7. Lietuvos Respublikos valstybės kontrolė;

9.8. Lietuvos Respublikos konkurencijos taryba;

9.9. Vyriausioji tarnybinės etikos komisija;

9.10. Žurnalistų etikos inspektoriaus tarnyba;

9.11. Lietuvos Respublikos vaiko teisių apsaugos kontrolieriaus įstaiga;

9.12. Lygių galimybių kontrolieriaus tarnyba;

9.13. Lietuvos Respublikos valstybinė kultūros paveldo komisija;

9.14. Valstybinė kainų ir energetikos kontrolės komisija;

9.15. Lietuvos Respublikos valstybės saugumo departamentas;

9.16. prokuratūros;

9.17. Lietuvos bankas;

9.18. Lietuvos radijo ir televizijos komisija;

9.19. Valstybės garantuojamos teisinės pagalbos tarnyba;

9.20. Muitinės departamentas prie Lietuvos Respublikos finansų ministerijos;

9.21. teritorinės muitinės;

9.22. Muitinės kriminalinė tarnyba;

9.23. Lietuvos Respublikos ryšių reguliavimo tarnyba;

9.24. Lietuvos statistikos departamentas;

9.25. Lietuvos vyriausiojo archyvaro tarnyba;

9.26. valstybės ir apskričių archyvai;

9.27. Valstybinė duomenų apsaugos inspekcija;

9.28. Narkotikų, tabako ir alkoholio kontrolės departamentas;

9.29. Valstybinė atominės energetikos saugos inspekcija;

9.30. Lošimų priežiūros tarnyba prie Lietuvos Respublikos finansų ministerijos;

9.31. Valstybinė maisto ir veterinarijos tarnyba;

9.32. Lietuvos Respublikos aplinkos ministerijos regionų aplinkos apsaugos departamentai;

9.33. Valstybinė saugomų teritorijų tarnyba prie Aplinkos ministerijos;

9.34. valstybiniai rezervatai, valstybiniai parkai, biosferos rezervatų direkcijų ir saugomų teritorijų valstybinio valdymo ir kontrolės įstaigos;

9.35. Civilinės aviacijos administracija;

9.36. Finansinių nusikaltimų tyrimo tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos;

9.37. Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos;

9.38. Lietuvos kariuomenės karo policija;

9.39. Lietuvos Respublikos akademinės etikos ir procedūrų kontrolieriaus tarnyba;

9.40. Kultūros paveldo departamentas prie Kultūros ministerijos;

9.41. Lietuvos Respublikos valstybinė kultūros paveldo komisija;

9.42. Lietuvos automobilių kelių direkcija prie Susisiekimo ministerijos;

9.43. Lietuvos geologijos tarnyba prie Aplinkos ministerijos;

9.44. Lietuvos metrologijos inspekcija;

9.45. Lietuvos Respublikos ginklų fondas prie Lietuvos Respublikos vidaus reikalų ministerijos;

9.46. Lietuvos Respublikos švietimo ir mokslo ministerija;

9.47. Studijų kokybės vertinimo centras;

9.48. Lietuvos saugios laivybos administracija;

9.49. Valstybinė miškų tarnyba;

9.50. Generalinė miškų urėdija prie Aplinkos ministerijos;

9.51. valstybės įmonės miškų urėdijos;

9.52. Mobilizacijos ir pilietinio pasipriešinimo departamentas prie Krašto apsaugos ministerijos;

9.53. Kibernetinio saugumo ir telekomunikacijų tarnyba prie Krašto apsaugos ministerijos;

9.54. Nacionalinė žemės tarnyba prie Žemės ūkio ministerijos;

9.55. Nacionalinis transplantacijos biuras prie Sveikatos apsaugos ministerijos;

9.56. Priešgaisrinės apsaugos ir gelbėjimo departamentas prie Vidaus reikalų ministerijos ir jam pavaldžios įstaigos;

9.57. Radiacinės saugos centras;

9.58. Vadovybės apsaugos departamentas prie Vidaus reikalų ministerijos;

9.59. Valstybės sienos apsaugos tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos ir jos struktūriniai padaliniai;

9.60. Valstybinė akreditavimo sveikatos priežiūros veiklai tarnyba prie Sveikatos apsaugos ministerijos;

9.61. Valstybinė augalininkystės tarnyba prie Žemės ūkio ministerijos;

9.62. Lietuvos Respublikos valstybinė darbo inspekcija prie Socialinės apsaugos ir darbo ministerijos;

9.63. Socialinių paslaugų priežiūros departamentas prie Socialinės apsaugos ir darbo ministerijos;

9.64. saugos ir paskirties reikalavimų valstybinės priežiūros institucijos;

9.65. Valstybės dokumentų technologinės apsaugos tarnyba prie Finansų ministerijos;

9.66. Valstybinė energetikos inspekcija prie Energetikos ministerijos;

9.67. Valstybinė geležinkelio inspekcija prie Susisiekimo ministerijos;

9.68. Valstybinė gyvulių veislininkystės priežiūros tarnyba prie Žemės ūkio ministerijos;

9.69. Valstybinė kelių transporto inspekcija prie Susisiekimo ministerijos;

9.70. Valstybinė kalbos inspekcija;

9.71. Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos;

9.72. teritorinės ligonių kasos;

9.73. Valstybinė mokesčių inspekcija prie Lietuvos Respublikos finansų ministerijos;

9.74. Valstybinė teritorijų planavimo ir statybos inspekcija prie Aplinkos ministerijos;

9.75. teritorijų planavimo valstybinės priežiūros institucijos;

9.76. Valstybinė vaistų kontrolės tarnyba prie Lietuvos Respublikos sveikatos apsaugos ministerijos;

9.77. Valstybinė vartotojų teisių apsaugos tarnyba;

9.78. Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos ir Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos teritoriniai skyriai;

9.79. Valstybinis turizmo departamentas prie Ūkio ministerijos;

9.80. Viešųjų pirkimų tarnyba;

9.81. Žuvininkystės tarnyba prie Lietuvos Respublikos žemės ūkio ministerijos;

9.82. savivaldybių administracijos;

9.83. valstybės įmonė Lietuvos prabavimo rūmai;

9.84. valstybės įmonė Registrų centras;

9.85. valstybės įmonė Turto bankas;

9.86. valstybės įmonė Klaipėdos valstybinio jūrų uosto direkcija;

9.87. Audito, apskaitos, turto vertinimo ir nemokumo valdymo tarnyba prie Lietuvos Respublikos finansų ministerijos;

9.88. Lietuvos Respublikos specialiųjų tyrimų tarnyba;

9.89. Viešojo saugumo tarnyba prie Vidaus reikalų ministerijos;

9.90. Lietuvos antstolių rūmai;

9.91. Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos;

9.92. viešoji įstaiga Audito ir apskaitos tarnyba;

9.93. savivaldybių vykdomųjų institucijų įgaliotos įstaigos ir įmonės;

9.94. valstybinę kelių transporto kontrolę atliekantys viešojo administravimo subjektai ar jų įgaliotos valstybės ar savivaldybių įstaigos ir įmonės;

9.95. statinių naudojimo priežiūros viešojo administravimo subjektai;

9.96. valstybės įmonė Valstybės žemės fondas;

9.97. Lietuvos Respublikos žemės ūkio ministerija;

9.98. valstybės įmonė Žemės ūkio informacijos ir kaimo verslo centras.

10. Informatikos ir ryšių departamento, kaip ANR tvarkytojo, funkcijos ir atsakomybė:

10.1. užtikrina ir atsako už ANR elektroninės informacijos tvarkymo teisėtumą ir saugų ANR elektroninės informacijos perdavimą elektroninių ryšių tinklais (automatiniu būdu);

10.2. užtikrina tinkamą ANR valdytojo patvirtintų Saugos nuostatų, ANR saugos politiką įgyvendinančių dokumentų, kitų dokumentų, susijusių su elektroninės informacijos sauga, rekomendacijų įgyvendinimą;

10.3. atlieka kitas Saugos nuostatų, ANR nuostatų, Bendrųjų saugos reikalavimų aprašo, Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo ir kitų teisės aktų nustatytas funkcijas, susijusias su ANR elektroninės informacijos sauga;

10.4. skiria ANR saugos įgaliotinį ir ANR administratorių;

10.5. suteikia teisę kitiems ANR tvarkytojams, turintiems jų reguliavimo sričiai priskirtų ANR tvarkytojų įstaigų – teritorinių, specializuotų, atskaitingų ir kitų (toliau – pavaldūs ANR tvarkytojai), administruoti savo bei pavaldžių ANR tvarkytojų ANR naudotojus.

11. Kiti ANR tvarkytojai atlieka ANR nuostatuose apibrėžtas funkcijas, taip pat:

11.1. kiekvienas paskiria savo ANR saugos įgaliotinį; jei ANR tvarkytojas turi pavaldžių ANR tvarkytojų, jis gali paskirti vieną saugos įgaliotinį, prižiūrintį ir kontroliuojantį ANR saugos politikos įgyvendinimą savo įstaigoje ir pavaldžių ANR tvarkytojų įstaigose;

11.2. teikia pasiūlymus ANR valdytojui, kaip tobulinti ANR elektroninės informacijos saugą;

11.3. užtikrina tinkamą ANR valdytojo priimtų teisės aktų ir rekomendacijų, susijusių su ANR elektroninės informacijos sauga, įgyvendinimą;

11.4. atlieka kitas Saugos nuostatų, ANR nuostatų, Bendrųjų saugos reikalavimų aprašo, Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo ir kitų teisės aktų nustatytas funkcijas, susijusias su ANR elektroninės informacijos sauga.

12. Visi ANR tvarkytojai užtikrina tvarkomos ANR elektroninės informacijos saugą tvarkytojo įstaigoje ir jiems pavaldžių ANR tvarkytojų įstaigose. ANR tvarkytojų vadovai atsako už reikiamų organizacinių, techninių ir programinių saugos priemonių įgyvendinimą, užtikrinimą ir

laikymąsi Saugos nuostatuose ir ANR saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka.

13. Informatikos ir ryšių departamento paskirtas ANR saugos įgaliotinis:

13.1. rengia ANR saugos politiką įgyvendinančių dokumentų projektus;

13.2. koordinuoja kitų ANR tvarkytojų paskirtų ANR saugos įgaliotinių veiklą, supažindina juos su Saugos nuostatais, ANR saugos politiką įgyvendinančiais dokumentais bei atsakomybe už juose nustatytų reikalavimų nesilaikymą;

13.3. koordinuoja ir prižiūri ANR elektroninės informacijos saugos politikos įgyvendinimą;

13.4. koordinuoja ANR elektroninės informacijos saugos ir kibernetinių incidentų (toliau – saugos incidentai) tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų incidentus, saugos incidentus, neteisėtas veikas, susijusias su elektroninės informacijos sauga;

13.5. teikia pasiūlymus Informatikos ir ryšių departamento direktoriui dėl:

13.5.1. ANR administratoriaus paskyrimo ir reikalavimų jam nustatymo;

13.5.2. Saugos nuostatų ir ANR saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar pripažinimo netekus galios;

13.5.3. ANR informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

13.6. teikia kitų ANR tvarkytojų paskirtiems ANR saugos įgaliotiniams, ANR administratoriui, ANR naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su ANR saugos politikos įgyvendinimu;

13.7. periodiškai, ne rečiau kaip kartą per kalendorinius metus, organizuoja kitų ANR tvarkytojų paskirtų ANR saugos įgaliotinių saugos mokymus, reguliariai jiems primena saugos problemas, teikia konsultacijas, prireikus rengia atmintines naujai priimtiems darbuotojams;

13.8. organizuoja ANR rizikos įvertinimą;

13.9. vykdo kitas Saugos nuostatų, ANR nuostatų, Bendrųjų saugos reikalavimų aprašo ir kitų teisės aktų nustatytas funkcijas.

14. Kitų ANR tvarkytojų paskirti saugos įgaliotiniai:

14.1. koordinuoja ir prižiūri ANR elektroninės informacijos saugos politikos įgyvendinimą tvarkytojo įstaigoje ir tvarkytojo įstaigos reguliavimo sričiai priskirtose kitose įstaigose, turinčiose ANR naudotojų darbo vietas;

14.2. teikia Informatikos ir ryšių departamento paskirtam ANR saugos įgaliotiniui siūlymus dėl:

14.2.1. Saugos nuostatų ir ANR saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar pripažinimo netekusiais galios;

14.2.2. ANR informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

14.2.3. saugos mokymų organizavimo;

14.3. teikia savo tvarkytojo įstaigos ir jos reguliavimo sričiai priskirtų kitų įstaigų ANR naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su ANR saugos politikos įgyvendinimu;

14.4. informuoja Informatikos ir ryšių departamento paskirtą ANR saugos įgaliotinį apie ANR saugos incidentus ir teikia siūlymus dėl jų pašalinimo;

14.5. supažindina savo tvarkytojo įstaigos ir jai pavaldžių ANR tvarkytojų, kurie nėra paskyrę saugos įgaliotinio, įstaigų ANR naudotojus su Saugos nuostatais ir ANR saugos politiką įgyvendinančiais dokumentais bei atsakomybe už šių reikalavimų nesilaikymą;

14.6. ne rečiau kaip kartą per kalendorinius metus organizuoja savo tvarkytojo įstaigos ir jai pavaldžių ANR tvarkytojų, kurie nėra paskyrę saugos įgaliotinio, įstaigų ANR naudotojų saugos mokymus, reguliariai jiems primena saugos problemas, teikia konsultacijas (elektroniniu paštu, telefonu, prireikus rengia atmintines naujai priimtiems darbuotojams ir pan.);

14.7. dalyvauja tiriant ANR tvarkytojo įstaigoje ir jai pavaldžių ANR tvarkytojų, kurie nėra paskyrę saugos įgaliotinio, įstaigose įvykusius saugos incidentus;

14.8. atlieka kitas Saugos nuostatuose ir kituose ANR saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas, susijusias su ANR elektroninės informacijos sauga.

15. ANR administratorius:

15.1. prižiūri ANR ir jo infrastruktūrą, užtikrina jos veikimą ir elektroninės informacijos saugą;

15.2. reguliariai tikrina (peržiūri) ANR įrangos sąranką ir jos būsenos rodiklius;

15.3. administruoja ANR naudotojus, išskyrus tuos ANR naudotojus, kurių administravimo teisės suteiktos kitiems ANR tvarkytojams pagal Saugos nuostatų 10.5 papunktį;

15.4. vykdo Informatikos ir ryšių departamento paskirto saugos įgaliotinio nurodymus ir pavedimus, susijusius su ANR saugos užtikrinimu, nuolat teikia jam informaciją apie saugą užtikrinančių pagrindinių komponentų būklę;

15.5. atlieka kitas Informatikos ir ryšių departamento direktoriaus pavestas, Bendrųjų saugos reikalavimų aprašo, ANR nuostatų ir kitų teisės aktų nustatytas funkcijas.

16. ANR elektroninė informacija tvarkoma ir jos sauga užtikrinama vadovaujantis:

16.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

16.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

16.3. Lietuvos Respublikos kibernetinio saugumo įstatymu;

16.4. Bendrųjų saugos reikalavimų aprašu;

16.5. Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo

gairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Klasifikavimo gairių aprašas);

16.6. ANR nuostatais;

16.7. Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais 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“;

16.8. Bendraisiais reikalavimais organizacinėms ir techninėms asmens duomenų saugumo priemonėms, patvirtintais 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);

16.9. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašu;

16.10. Lietuvos standartais LST ISO/IEC 27001:2013, LST ISO/IEC 27002:2014, taip pat kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais, apibūdinančiais informacijos saugos valdymą ir saugų duomenų tvarkymą;

16.11. kitais teisės aktais, reglamentuojančiais elektroninės informacijos tvarkymo teisėtumą ir elektroninės informacijos saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

17. ANR tvarkoma elektroninė informacija priskiriama ypatingos svarbos elektroninės informacijos kategorijai vadovaujantis Klasifikavimo gairių aprašo 7.2 ir 7.5 papunkčiuose nustatytais kriterijais.

18. Atsižvelgiant į ANR tvarkomos elektroninės informacijos svarbos kategoriją ir vadovaujantis Klasifikavimo gairių aprašo 12.1 papunkčiu, ANR priskiriamas pirmajai kategorijai.

19. ANR asmens duomenų tvarkymas automatiniu būdu priskirtinas antrajam saugumo lygiui vadovaujantis Bendrųjų reikalavimų asmens duomenų saugumo priemonėms 11.2 papunkčio nuostata.

20. Informatikos ir ryšių departamento paskirtas ANR saugos įgaliotinis, atsižvelgdamas į VRM išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius

„Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja ANR rizikos įvertinimą ir parengia rizikos įvertinimo ataskaitą; prireikus jis gali organizuoti neeilinį rizikos įvertinimą.

21. ANR rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausi rizikos veiksniai:

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

21.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis ANR, duomenų pakeitimas ir sunaikinimas, duomenų perdavimo tinklų veiklos trikdymai, fizinio saugumo pažeidimai, vagystės ir kita);

21.3. 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.

22. ANR valdytojas, atsižvelgdamas į ANR rizikos įvertinimo ataskaitą, prireikus tvirtina Informatikos ir ryšių departamento parengtą rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

23. ANR saugos priemonės parenkamos įvertinus galimus rizikos veiksnius ANR duomenų vientisumui, konfidencialumui ir prieinamumui.

24. Siekdamas užtikrinti Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatytų reikalavimų įgyvendinimo organizavimą ir įgyvendinimo kontrolę, Informatikos ir ryšių departamento paskirtas ANR saugos įgaliotinis ne rečiau kaip kartą per metus organizuoja ANR informacinių technologijų saugos atitikties vertinimą, kurio metu:

24.1. įvertinama realios ANR elektroninės informacijos saugos situacijos atitiktis Saugos nuostatų, saugos politiką įgyvendinančių dokumentų reikalavimams, Organizacinių ir techninių kibernetinio saugumo reikalavimų ir kitų teisės aktų reikalavimams;

24.2. patikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų ANR naudotojų kompiuterizuotų darbo vietų bei visų tarnybinių stočių įdiegta programinė įranga ir jos sąranka;

24.3. patikrinama (įvertinama) ANR naudotojams ir administratoriams suteiktų teisių atitiktis vykdomoms funkcijoms;

24.4. įvertinamas pasirengimas užtikrinti ANR veiklos tęstinumą įvykus saugos incidentui.

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

26. Atlikus ANR informacinių technologijų saugos atitikties vertinimą, Informatikos ir ryšių departamento paskirtas ANR saugos įgaliotinis rengia pastebėtų trūkumų šalinimo planą, kurį tvirtina, atsakingus vykdytojus paskiria ir nustatytų trūkumų šalinimo įgyvendinimo terminus nustato ANR valdytojas.

27. Pagrindiniai elektroninės informacijos saugos priemonių parinkimo principai yra šie:

27.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

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

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

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

28. Programinės įrangos, skirtos ANR apsaugoti nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir panašiai), naudojimo nuostatos ir jos atnaujinimo reikalavimai:

28.1. ANR tarnybinėse stotyse ir kompiuterizuotose darbo vietose turi būti naudojamos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės, nuolat ieškančios ir blokuojančios kenksmingą programinę įrangą (virusų, šnipinėjimo programinę įrangą ir kt.), kurios turi būti reguliariai atnaujinamos automatiniu būdu ne rečiau kaip kartą per 24 valandas;

28.2. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

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

29.1. ANR darbui gali būti naudojama tik legali ir patikrinta programinė įranga;

29.2. programinė įranga atnaujinama laikantis gamintojo reikalavimų;

29.3. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka ANR administratorius (administratoriai).

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

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

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

30.3. turi būti naudojamos turinio filtravimo sistemos.

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

31.1. ANR naudotojų, jų vykdytų užklausų ir peržiūrėtų užklausų rezultatų duomenys tvarkomi Vidaus reikalų informacinės sistemos naudotojų administravimo posistemėje Lietuvos Respublikos 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;

31.2. tiesioginė prieiga prie ANR elektroninės informacijos suteikiama įgyvendinus ANR naudotojų administravimo taisyklėse nurodytas ANR naudotojų autentifikavimo priemones. Tiesioginė prieiga prie ANR užtikrinama automatiniu būdu ištisą parą, darbo ir poilsio dienomis;

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

31.4. ANR elektroninė informacija, perduodama ne per ANR tvarkytojams priklausančias duomenų perdavimo linijas, privalo būti šifruojama;

31.5. įgyvendinamos priemonės, užtikrinančios, kad ANR nuostatų 15.2.4 papunktyje nurodytas veido atvaizdas būtų perduodamas tik ANR naudotojams, turintiems teisę juos gauti ir tik tais atvejais, kai atliekant jų tiesiogines funkcijas būtina nustatyti ir (ar) patikslinti administracinėn atsakomybėn traukiamo asmens tapatybę.

32. ANR elektroninės informacijos perdavimui naudojamas Vidaus reikalų telekomunikacinis tinklas ir Saugus valstybinis duomenų perdavimo tinklas.

33. ANR naudotojams, savo tiesioginėms funkcijoms atlikti naudojantiems nešiojamus kompiuterius ANR elektroninės informacijos perdavimui kompiuterių tinklais ne savo darbo vietoje, šiuose kompiuteriuose turi būti naudojamas kompiuterio įjungimo slaptažodis, papildomas ANR naudotojo tapatybės patvirtinimas ir elektroninės informacijos šifravimas.

34. ANR naudotojams, kuriems būtinas prisijungimas tiesioginėms funkcijoms atlikti iš nutolusios darbo vietos, gali būti suteikiama nuotolinio prisijungimo prie ANR galimybė:

34.1. 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);

34.2. prie ANR prisijungiama nuotoliniu būdu naudojant interneto naršyklę (HTTPS protokolą);

34.3. ANR duomenų teikėjams ar gavėjams nuotolinio prisijungimo prie ANR galimybė suteikiama tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas.

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

35.1. ANR elektroninės informacijos kopijos turi būti daromos automatiškai kiekvieną dieną. Prireikus jas atkurti turi teisę ANR administratorius;

35.2. atkūrimas iš elektroninės informacijos kopijų privalo būti išbandomas;

35.3. elektroninės informacijos kopijos turi būti saugomos kitoje patalpoje nei ANR tarnybinės stotys.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

36. ANR 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 duomenų tvarkymą, privalo tobulinti kvalifikaciją elektroninės informacijos saugos srityje.

37. ANR saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

38. ANR administratorius privalo išmanyti pagrindinius elektroninės informacijos saugos, ir darbo su duomenų perdavimo tinklais principus, turėti sisteminių programinių priemonių administravimo ir priežiūros patirties, mokėti administruoti ir prižiūrėti duomenų bazes, gebėti užtikrinti techninės ir programinės įrangos nepertraukiamą funkcionavimą, stebėti techninės ir programinės įrangos veikimą, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, sutrikimų diagnostiką ir šalinimą, turėti sisteminių programinių priemonių (*Windows, Unix, Oracle*) administravimo ir priežiūros patirties.

39. ANR naudotojai privalo:

39.1. turėti atitinkamą kvalifikaciją (informacinių technologijų vartotojų kvalifikacijos kursai, pradinis saugaus darbo su duomenimis mokymas, ECDL (Europos kompiuterio vartotojo pažymėjimas) vartotojo sertifikatas ar pan.) ir patirties (dirbant su atitinkamomis operacinėmis sistemomis, taikomosiomis programomis ir pan.);

39.2. būti susipažinę su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, kitais teisės aktais, reglamentuojančiais asmens duomenų tvarkymą ir ANR duomenų saugą;

39.3. būti pasirašę pasižadėjimą saugoti asmens duomenų ir kitų ANR duomenų paslaptį;

39.4. nuolat kelti kvalifikaciją kvalifikacijos kėlimo kursuose, saugaus darbo su duomenimis seminaruose.

40. ANR naudotojams ne rečiau kaip kartą per kalendorinius metus turi būti rengiami elektroninės informacijos saugosmokymai, įvairiais būdais primenama apie saugos problematiką (pvz., priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės ir pan.). Saugos mokymai organizuojami periodiškai, mokymus organizuoja ir jų efektyvumą vertina Informatikos ir ryšių departamento paskirtas ANR saugos įgaliotinis kartu su kitų ANR tvarkytojų paskirtais ANR saugos įgaliotiniais.

V SKYRIUS
ANR NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

41. Tvarkyti ANR elektroninę informaciją gali tik ANR naudotojai, susipažinę su Saugos nuostatais, ANR saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, bei atsakomybe už saugos dokumentų nuostatų pažeidimus, ir raštu sutikę laikytis saugos dokumentuose nustatytų reikalavimų. Pakartotinis supažindinimas yra vykdomas pasikeitus minėtiems dokumentams ir teisės aktams.

42. Už ANR naudotojų supažindinimą su šiais Saugos nuostatais ir ANR saugos politiką įgyvendinančiais dokumentais pagal kompetenciją yra atsakingi Informatikos ir ryšių departamento paskirtas ANR saugos įgaliotinis ir kitų ANR tvarkytojų paskirti ANR saugos įgaliotiniai.

43. ANR Saugos nuostatai ir ANR saugos politiką įgyvendinantys dokumentai skelbiami ANR valdytojo interneto svetainėje.

44. ANR naudotojai su Saugos nuostatais ir ANR saugos politiką įgyvendinančiais dokumentais bei atsakomybe už jų reikalavimų nesilaikymą supažindinami pasirašytinai.

45. Saugos nuostatai ir ANR saugos politiką įgyvendinantys dokumentai iš esmės turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per kalendorinius metus. Šie saugos dokumentai turi būti persvarstomi (peržiūrimi) atlikus rizikos veiksnių analizę ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams.

Informatikos ir ryšių departamento paskirtas saugos įgaliotinis atsakingas, kad ANR naudotojai būtų informuoti apie jų pakeitimą ir (ar) pripažinimą netekusiais galios.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

46. ANR tvarkytojai, ANR saugos įgaliotiniai, ANR administratorius ir ANR naudotojai, pažeidę Saugos nuostatų ar kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų reikalavimus, atsako Lietuvos Respublikos įstatymų ir kitų teisės aktų nustatyta tvarka.

Priedo pakeitimai:
Nr. 1V-623, 2017-09-08, paskelbta TAR 2017-09-08, i. k. 2017-14383

Pakeitimai:

1.
Lietuvos Respublikos vidaus reikalų ministerija, Įsakymas
Nr. 1V-623, 2017-09-08, paskelbta TAR 2017-09-08, i. k. 2017-14383
Dėl vidaus reikalų ministro įsakymo „Dėl Lietuvos Respublikos vidaus reikalų ministro 2015 m. spalio 5 d. įsakymo Nr. 1V-781 „Dėl Administracinių teisės pažeidimų registro duomenų saugos nuostatų patvirtinimo“ pakeitimo