LIETUVOS RESPUBLIKOS KRAŠTO APSAUGOS MINISTRAS

ĮSAKYMAS
DĖL VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ ATITIKTIES ELEKTRONINĖS INFORMACIJOS SAUGOS REIKALAVIMAMS STEBĖSENOS SISTEMOS NUOSTATŲ PATVIRTINIMO

2018 m. gruodžio 11 d. Nr. V-1183
Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 8 straipsniu, 30 straipsnio 1 dalimi, 6 straipsnio 4 dalies 1 punktu, 43^1 straipsniu ir Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“, 11 punktu:

1. T v i r t i n u Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatus (pridedama).

2. S k i r i u Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos Informacijos saugumo departamento direktoriaus pavaduotoją Aidą Čipkuvienę Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos duomenų valdymo įgaliotine.

Krašto apsaugos ministras Raimundas Karoblis

PATVIRTINTA
Lietuvos Respublikos krašto apsaugos
ministro 2018 m. gruodžio 11 d.
įsakymu Nr. V-1183

VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ ATITIKTIES ELEKTRONINĖS INFORMACIJOS SAUGOS REIKALAVIMAMS STEBĖSENOS SISTEMOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatai (toliau – Nuostatai) nustato valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos (toliau – ARSIS) steigimo pagrindą, tikslą, uždavinį, funkcijas, organizacinę, informacinę ir funkcinę struktūras, ARSIS duomenų teikimo ir naudojimo tvarką, ARSIS duomenų saugą, ARSIS finansavimo, modernizavimo ir likvidavimo tvarką.

2. ARSIS steigimo pagrindas – Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 6 straipsnio 4 dalies 1 punktas, 43^1 straipsnio 1 dalis.

3. ARSIS tikslas – informacinių technologijų priemonėmis atlikti valstybės informacinių išteklių (toliau – informaciniai ištekliai) atitikties teisės aktų nustatytiems elektroninės informacijos saugos reikalavimams (toliau – saugos reikalavimai) stebėseną.

4. ARSIS uždavinys – automatizuoti duomenų apie saugos reikalavimų įgyvendinimą informaciniuose ištekliuose tvarkymo, valstybės ir kitų informacinių sistemų, valstybės ir žinybinių registrų (toliau – informacinės sistemos ir registrai) rizikos vertinimo, atitikties saugos reikalavimams priežiūros, informacinių sistemų ir registrų valdytojų informavimo apie jų valdomiems informaciniams ištekliams taikomus saugos reikalavimus ir elektroninės informacijos saugos rizikas procesus.

5. ARSIS funkcijos:

5.1. kaupti, saugoti, apdoroti, sisteminti ir kitaip tvarkyti duomenis apie:

5.1.1. saugos reikalavimus ir jų įgyvendinimą valdant ir tvarkant informacinius išteklius;

5.1.2. informacinių sistemų ir registrų rizikos vertinimus ir jos valdymą;

5.1.3. informacinių išteklių neatitikimo saugos reikalavimams šalinimą ir informacinių sistemų ir registrų valdytojų šiuo tikslu vykdomas saugos stiprinimo ir tobulinimo priemones;

5.1.4. saugumo įvykius;

5.2. informuoti informacinių sistemų ir registrų valdytojus ir tvarkytojus apie jų valdomiems ir (ar) tvarkomiems informaciniams ištekliams taikomus saugos reikalavimus, jų įgyvendinimo būdus, elektroninės informacijos saugos rizikas ir jų valdymo būdus;

5.3. administruoti ARSIS naudotojus, kontroliuoti jų veiksmus.

6. Asmens duomenų tvarkymo ARSIS tikslas – identifikuoti ARSIS naudotojus ir kontroliuoti jų veiksmus.

7. ARSIS kuriama ir tvarkoma vadovaujantis:

7.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

7.2. Lietuvos Respublikos kibernetinio saugumo įstatymu;

7.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (toliau – Asmens duomenų teisinės apsaugos įstatymas);

7.4. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Bendrasis duomenų apsaugos reglamentas);

7.5. Asmens duomenų tvarkymo ir duomenų subjektų teisių įgyvendinimo krašto apsaugos sistemoje taisyklėmis, patvirtintomis Lietuvos Respublikos krašto apsaugos ministro 2015 m. gruodžio 3 d. įsakymu Nr. V-1253 „Dėl Asmens duomenų tvarkymo ir duomenų subjektų teisių įgyvendinimo krašto apsaugos sistemoje taisyklių patvirtinimo“;

7.6. Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“ (toliau − Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas);

7.7. Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa, patvirtinta Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimu Nr. 796 „Dėl Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“;

7.8. 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“;

7.9. Bendrųjų elektroninės informacijos saugos reikalavimų 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 – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas);

7.10. Nuostatais.

8. Nuostatuose vartojamos sąvokos apibrėžtos Nuostatų 7 punkte nurodytuose teisės aktuose.

II SKYRIUS
ARSIS ORGANIZACINĖ STRUKTŪRA

9. ARSIS valdytoja ir ARSIS kaupiamų asmens duomenų valdytoja yra Lietuvos Respublikos krašto apsaugos ministerija.

10. ARSIS tvarkytojas ir ARSIS kaupiamų asmens duomenų tvarkytojas yra Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos.

11. ARSIS valdytoja atlieka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme nustatytas funkcijas, turi šiame įstatyme nustatytas teises ir pareigas.

12. ARSIS valdytoja, kaip asmens duomenų valdytoja, atlieka Bendrajame duomenų apsaugos reglamente nustatytas asmens duomenų valdytojo funkcijas, turi šiame reglamente nurodytas asmens duomenų valdytojo teises ir pareigas.

13. ARSIS asmens duomenų tvarkytojas įgyvendina asmens duomenų tvarkytojo funkcijas pagal Bendrojo duomenų apsaugos reglamento 28 straipsnį. ARSIS tvarkytojas atlieka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme nustatytas funkcijas, turi šiame įstatyme nustatytas teises ir pareigas, taip pat:

13.1. ARSIS saugos dokumentuose nustatyta tvarka užtikrina reikiamas administracines, technines ir organizacines ARSIS tvarkomų duomenų saugos priemones ir kontroliuoja, kaip laikomasi tokių priemonių;

13.2. atlieka centralizuotą ARSIS naudotojų administravimą;

13.3. teikia ARSIS valdytojui pasiūlymus dėl ARSIS tobulinimo, jai eksploatuoti, prižiūrėti ir plėsti skirtų techninių, programinių priemonių įsigijimo, organizuoja jų įdiegimą, modernizavimą, priežiūrą;

13.4. atlieka kitus Nuostatuose nustatytus veiksmus.

14. ARSIS tvarkytojas, kaip asmens duomenų tvarkytojas, atlieka Bendrajame duomenų apsaugos reglamente nustatytas funkcijas, turi šiame reglamente nurodytas teises ir pareigas.

15. ARSIS duomenų teikėjai yra:

15.1. Informacinės visuomenės plėtros komitetas prie Lietuvos Respublikos susisiekimo ministerijos, kuris teikia į ARSIS:

15.1.1. registrų ir valstybės informacinių sistemų registro (toliau – RISR) duomenis;

15.1.2. valstybės informacinių išteklių sąveikumo platformos (toliau – VIISP) duomenis;

15.2. valstybės informacinių sistemų, valstybės ir žinybinių registrų valdytojai ir (ar) tvarkytojai, kurie teikia duomenis, nekaupiamus valstybės informacinėse sistemose ir registruose (toliau – pirminiai duomenys);

15.3. institucijų vidaus administravimui skirtų informacinių sistemų valdytojai ir (ar) tvarkytojai, kurie teikia pirminius duomenis.

III SKYRIUS
ARSIS INFORMACINĖ STRUKTŪRA

16. ARSIS duomenų bazėje kaupiami šie duomenys:

16.1. informacinių sistemų ir registrų duomenys:

16.1.1. informacinės sistemos ar registro pavadinimas;

16.1.2. įregistravimo RISR data;

16.1.3. RISR objekto tipas;

16.1.4. valdytojo duomenys:

16.1.4.1. institucijos pavadinimas;

16.1.4.2. juridinio asmens kodas;

16.1.4.3. buveinės adresas;

16.1.4.4. interneto svetainės adresas;

16.1.5. tvarkytojo duomenys:

16.1.5.1. institucijos pavadinimas;

16.1.5.2. juridinio asmens kodas;

16.1.5.3. buveinės adresas;

16.1.5.4. interneto svetainės adresas;

16.1.6. nuoroda į informacinės sistemos ar registro kortelę RISR;

16.1.7. informacinės sistemos ar registro kategorija;

16.1.8. asmens duomenų saugumo lygis;

16.1.9. valstybės informacinio ištekliaus rūšis;

16.2. saugos reikalavimų duomenys:

16.2.1. teisės akto pavadinimas;

16.2.2. teisės akto rūšis;

16.2.3. teisės aktą priėmusios institucijos pavadinimas;

16.2.4. teisės akto priėmimo data;

16.2.5. teisės akto numeris;

16.2.6. teisės akto oficialaus paskelbimo šaltinis;

16.2.7. teisės akto įsigaliojimo data;

16.2.8. nuoroda į teisės aktą internete;

16.2.9. teisės akto galiojimo būsena;

16.2.10. reikalavimo punkto teisės akte numeris;

16.2.11. reikalavimo turinys;

16.2.12. reikalavimo taikymo sritis (pagal informacinio ištekliaus rūšį, kategoriją, elektroninės informacijos svarbą, asmens duomenų saugumo lygį);

16.2.13. informaciniai ištekliai, kuriems netaikomas reikalavimas;

16.2.14. reikalavimo įgyvendinimo būdas;

16.2.15. reikalavimui taikytinos saugos priemonės;

16.2.16. reikalavimo įgyvendinimo brandos lygis;

16.2.17. reikalavimo neįgyvendinimo keliama rizika;

16.2.18. tipiniai reikalavimo įgyvendinimo klausimai;

16.2.19. teisės aktuose apibrėžtos sąvokos;

16.3. saugos reikalavimų įgyvendinimo informaciniuose ištekliuose duomenys:

16.3.1. informacinių technologijų saugos auditų duomenys:

16.3.1.1. audito pavadinimas;

16.3.1.2. audito tipas;

16.3.1.3. auditą atlikusio subjekto pavadinimas;

16.3.1.4. auditą atlikusio asmens vardas ir pavardė, pareigos;

16.3.1.5. klausimyno užpildymo terminas;

16.3.1.6. klausimyno pateikimo ARSIS naudotojui data;

16.3.1.7. informacinės sistemos ar registro pavadinimas;

16.3.1.8. audito ataskaita;

16.3.1.9. audito atlikimo būsena;

16.3.1.10. atitikties reikalavimui įvertinimo lygis;

16.3.1.11. atitikties reikalavimui vertinimo komentaras;

16.3.1.12. atitikties reikalavimui įrodymai;

16.4. bendrieji saugos priemonių duomenys:

16.4.1. saugos priemonės pavadinimas;

16.4.2. saugos priemonės aprašas;

16.4.3. mažinamo rizikos veiksnio pavadinimas;
16.4.4. saugos priemonės įdiegimo darbo sąnaudų trukmė;
16.4.5. darbo sąnaudų aprašas;
16.4.6. saugos priemonei įdiegti reikalingų investicijų dydis;
16.4.7. investicijų aprašas;
16.5. saugos priemonių įgyvendinimo projektų duomenys:
16.5.1. projekto pavadinimas;
16.5.2. projektų grupės pavadinimas;
16.5.3. projekto aprašas;
16.5.4. projekto pradžios data;
16.5.5. projekto pabaigos data;
16.5.6. projektui įgyvendinti reikalingų išteklių duomenys:
16.5.6.1. projektui įgyvendinti reikalingų investicijų dydis;
16.5.6.2. projekto įgyvendinimo darbo sąnaudos;
16.5.6.3. projekto įgyvendinimo aprašas;
16.5.7. projektu mažinami rizikos veiksniai;
16.5.8. projektu šalinamos neatitiktys teisės aktų reikalavimams;
16.5.9. projekto rezultatų pasiekimo lygis;
16.5.10. projekto kontrolės taškų pasiekimo lygis;
16.5.11. kaštų plano vykdymo indikatoriaus vertė;
16.5.12. laiko plano vykdymo indikatorius vertė;
16.6. rizikos įvertinimo duomenys:
16.6.1. bendrieji rizikos įvertinimo duomenys:
16.6.1.1. rizikos įvertinimo pateikimo data;
16.6.1.2. rizikos įvertinimą atlikusio subjekto pavadinimas;
16.6.1.3. rizikos įvertinimą atlikusio asmens vardas ir pavardė, pareigos;
16.6.1.4. rizikos įvertinimo pavadinimas;
16.6.1.5. rizikos įvertinimo ataskaita;
16.6.1.6. rizikos įvertinimo pateikimo būdas;
16.6.1.7. informacinės sistemos ir registrai, kurių rizikos įvertinimas atliktas;
16.6.1.8. rizikos įvertinimo pateikimo būsena;
16.6.2. informacinio ištekliaus kritiškumo duomenys:
16.6.2.1. poveikio konfidencialumui lygis ir aprašas;
16.6.2.2. poveikio vientisumui lygis ir aprašas;
16.6.2.3. poveikio pasiekiamumui lygis ir aprašas;

16.6.3. grėsmių vertinimo duomenys:

16.6.3.1. grėsmės pavadinimas;

16.6.3.2. grėsmės tikimybė;

16.6.3.3. pažeidžiamumo aprašas;

16.6.3.4. grėsmės tikimybę padedantys nustatyti klausimai;

16.6.3.5. taikytinos saugos priemonės pavadinimas;

16.6.4. specialūs rizikos įvertinimo duomenys:

16.6.4.1. rizikos pavadinimas;

16.6.4.2. rizikos lygis;

16.6.4.3. rizikos priimtinumas;

16.6.4.4. likutinės rizikos lygis;

16.6.5. rizikos klasifikatoriaus duomenys:

16.6.5.1. rizikos veiksnio pavadinimas;

16.6.5.2. rizikos veiksnio aprašas;

16.6.5.3. rizikos veiksnių grupės pavadinimas;

16.6.5.4. rizikos veiksnio paveikiamas informacinio ištekliaus saugumo komponentas: konfidencialumas, vientisumas ir (arba) pasiekiamumas;

16.6.5.5. tikėtinas rizikos veiksnio pasireiškimo dažnis;

16.6.5.6. tikėtinas rizikos veiksnio sukeliamos žalos lygis;

16.6.5.7. siūlomos saugos priemonės;

16.7. duomenys apie saugumo įvykius:

16.7.1. įvykio pavadinimas;

16.7.2. įvykio aprašas;

16.7.3. įvykio tipas;

16.7.4. įvykio užfiksavimo data ir laikas;

16.7.5. su įvykiu susijusio informacinio ištekliaus pavadinimas;

16.7.6. įvykį teikiančios programinės įrangos pavadinimas;

16.8. ARSIS tvarkomi asmens duomenys:

16.8.1. už informacinių sistemų ar registrų duomenų tvarkymą paskirtų atsakingų asmenų (ARSIS naudotojų) duomenys:

16.8.1.1. naudotojo paskyros vardas;

16.8.1.2. atsakingo asmens vardas;

16.8.1.3. atsakingo asmens pavardė;

16.8.1.4. elektroninio pašto adresas;

16.8.1.5. asmens kodas / valstybės tarnautojo kodas;

16.8.1.6. institucija;

16.8.1.7. pareigos;

16.8.1.8. telefono ryšio numeris;

16.8.1.9. adresas;

16.8.1.10. vaidmuo;

16.8.2. duomenų valdymo įgaliotinio duomenys:

16.8.2.1. vardas;

16.8.2.2. pavardė;

16.8.2.3. pareigos;

16.8.3. saugos įgaliotinio duomenys:

16.8.3.1. vardas;

16.8.3.2. pavardė;

16.8.3.3. pareigos;

16.9. institucijų duomenys:

16.9.1. pavadinimas;

16.9.2. juridinio asmens kodas;

16.9.3. buveinės adresas;

16.9.4. interneto svetainės adresas;

16.9.5. institucijos pavaldumas;

16.10. ARSIS klasifikatoriai:

16.10.1. informacinio ištekliaus kategorija;

16.10.2. informacinio ištekliaus tipas;

16.10.3. informacinio ištekliaus asmens duomenų saugumo lygis;

16.10.4. teisės akto rūšis;

16.10.5. teisės akto galiojimo būsena;

16.10.6. reikalavimo įgyvendinimo būdas;

16.10.7. reikalavimo įgyvendinimo brandos lygis;

16.10.8. audito tipas;

16.10.9. audito atlikimo būsena;

16.10.10. atitikties reikalavimui įvertinimo lygis;

16.10.11. rizikos įvertinimo pateikimo būdas;

16.10.12. rizikos įvertinimo pateikimo būsena;

16.10.13. informacinio ištekliaus kritiškumas (poveikio konfidencialumui, vientisumui, prieinamumui lygis);

16.10.14. grėsmės tikimybė;

16.10.15. rizikos lygis;

16.10.16. rizikos priimtinumas;

16.10.17. likutinės rizikos lygis;

16.10.18. tikėtinas rizikos veiksnio pasireiškimo dažnis;

16.10.19. tikėtinas rizikos veiksnio sukeliamos žalos lygis;

16.10.20. saugos priemonių grupė;

16.10.21. saugumo įvykio tipas.

17. Nuostatų 16.7 papunktyje nurodyti duomenys teikiami, jei atitinkamos informacinės sistemos ir registrų valdytojas ar tvarkytojas disponuoja techninėmis priemonėmis tokius duomenis leidžiamosios kreipties būdu teikti ARSIS.

18. ARSIS duomenims tvarkyti naudojami šių informacinių sistemų ir registrų duomenų teikėjų pateikti duomenys:

18.1. RISR – Nuostatų 16.1.1–16.1.6, 16.8.2 ir 16.9.1–16.9.4 papunkčiuose nurodyti duomenys;

18.2. VIISP – asmens kodas / valstybės tarnautojo kodas;

18.3. valstybės informacinių sistemų, valstybės ir žinybinių registrų valdytojų ir (ar) tvarkytojų – Nuostatų 16.1.7−16.1.9, 16.8.3 ir 16.3−16.7 papunkčiuose nurodyti pirminiai duomenys;

18.4. institucijų vidaus administravimui skirtų informacinių sistemų valdytojų ir (ar) tvarkytojų − Nuostatų 16.1 (išskyrus duomenis, nurodytus 16.1.6 papunktyje), 16.8.2.1–16.8.3.3 ir 16.3−16.7 papunkčiuose nurodyti pirminiai duomenys.

IV SKYRIUS
ARSIS FUNKCINĖ STRUKTŪRA

19. ARSIS funkcinę struktūrą sudaro:

19.1. duomenų įvedimo ir gavimo posistemis, kurio funkcijos:

19.1.1. įvesti, pateikti į ARSIS informacinių išteklių atitikties saugos reikalavimams duomenis ir juos gauti;

19.1.2. kontroliuoti įvedamų ir pateikiamų duomenų išsamumą ir kokybę;

19.2. informacinių išteklių posistemis, kurio funkcija – tvarkyti duomenis apie informacines sistemas ir registrus, jų valdytojus, tvarkytojus, tarpusavio ryšius ir taikytinus saugos reikalavimus;

19.3. elektroninės informacijos saugos reikalavimų posistemis, kurio funkcija – tvarkyti duomenis, apibūdinančius saugos reikalavimus, jų tarpusavio ryšius, taikymo sritis ir įgyvendinimo būdus;

19.4. ataskaitų ir vizualizavimo posistemis, kurio funkcijos:

19.4.1. stebėti, įvairiomis priemonėmis analizuoti ARSIS duomenis ir pateikti ataskaitas (atitikties vertinimo, rizikos įvertinimo ir kitas);

19.4.2. pateikti informaciją apie informacinių išteklių saugos būklę naudojant įvairius grafinius būdus – diagramas, lenteles ir kita;

19.5. audito posistemis, kurio funkcijos:

19.5.1. tvarkyti informacinių išteklių saugos auditų duomenis;

19.5.2. analizuoti ir vertinti informacinių išteklių atitiktį saugos reikalavimams ir šią atitiktį pagrindžiančius duomenis;

19.5.3. vertinti saugos reikalavimų neatitikties riziką ir teikti rekomendacijas dėl informacinių išteklių saugos audito tikslingumo ir (ar) saugos reikalavimų taikymo tikslingumo;

19.6. automatinės stebėsenos posistemis, kurio funkcija – teikti į ARSIS informacijos saugumo įvykių duomenis leidžiamosios kreipties būdu;

19.7. rizikos vertinimo posistemis, kurio funkcijos:

19.7.1. atlikti ir atvaizduoti rizikų analizę;

19.7.2. apskaičiuoti ir sekti informacinių išteklių riziką;

19.7.3. valdyti rizikų grėsmių klasifikatorių;

19.8. informacinių išteklių saugos tobulinimo projektų posistemis, kurio funkcijos:

19.8.1. valdyti informacinių išteklių neatitikimo saugos reikalavimams šalinimą;

19.8.2. valdyti informaciniams ištekliams kylančių rizikų mažinimą ir šalinimą;

19.8.3. stebėti ir kontroliuoti informacinių išteklių saugos tobulinimo projektų įgyvendinimą;

19.9. administravimo posistemis, kurio funkcijos:

19.9.1. administruoti ARSIS naudotojus ir jų prieigos teises;

19.9.2. tvarkyti ARSIS sąrankas (konfigūracijas);

19.9.3. tvarkyti ARSIS klasifikatorius;

19.9.4. valdyti ARSIS naudotojų darbo sekas;

19.9.5. valdyti ARSIS duomenų kokybę;

19.9.6. kontroliuoti ARSIS naudotojų veiksmus;

19.9.7. administruoti ARSIS duomenų saugos priemones.

V SKYRIUS
ARSIS DUOMENŲ TEIKIMAS IR NAUDOJIMAS

20. Informacinių sistemų ir registrų valdytojams ir (ar) tvarkytojams, nurodytiems Nuostatų 15.2 ir 15.3 papunkčiuose, teikiami duomenys apie jų valdomų ir (ar) tvarkomų informacinių išteklių atitiktį saugos reikalavimams, rizikas, taikytinas saugos priemones ir jų diegimą bei informacijos saugumo įvykius interaktyviai (per interneto naršyklę) ir (arba) leidžiamosios kreipties būdu (sąsaja tarp sistemų). Šiame punkte nurodytiems duomenų gavėjams ARSIS duomenys teikiami nuolat, nesudarant duomenų teikimo sutarties.

21. Duomenų gavėjams, nenurodytiems Nuostatų 20 punkte, ARSIS duomenys teikiami pagal duomenų teikimo sutartis (daugkartinio teikimo atvejais) arba duomenų gavėjo prašymu (vienkartinio teikimo atvejais). Kai duomenys teikiami duomenų gavėjo prašymu, prašyme turi būti nurodytas prašomų duomenų teikimo ir gavimo teisinis pagrindas, jų naudojimo tikslas, teikimo būdas, apimtis, gavimo būdai, teikiamų duomenų formatas. Kai duomenys teikiami duomenų gavėjui pagal duomenų teikimo sutartį, sutartyje turi būti nustatyta ARSIS duomenų teikimo ir gavimo teisinis pagrindas, jų naudojimo tikslas, sąlygos ir tvarka, teikiamų duomenų apimtis.

22. Detalūs Lietuvos standarto LST ISO/IEC 27001 ir LST ISO/IEC 27002 duomenys ARSIS duomenų gavėjams teikiami tik tuo atveju, jei duomenų gavėjai Nuostatų 47 punkte nustatyta tvarka nurodė, kad turi teisę naudotis šiais standartais.

23. ARSIS duomenys yra vieši, tačiau neskelbiami. Asmens duomenys naudojami vadovaujantis Bendruoju duomenų apsaugos reglamentu.

24. ARSIS duomenys duomenų gavėjams teikiami neatlygintinai.

25. ARSIS duomenys duomenų gavėjams teikiami tokio turinio ir tokios formos, kokie yra naudojami ARSIS, ir nereikia duomenų apdoroti papildomai. Jeigu ARSIS teikiamų duomenų forma ir turinys neatitinka ARSIS duomenų gavėjo poreikių, jei yra techninės galimybės, ARSIS tvarkytojas gali pateikti duomenis kita forma, kuri turi būti nustatyta duomenų teikimo sutartyje.

26. ARSIS tvarkytojas, nustatęs į ARSIS pateiktų duomenų, informacijos, dokumentų ir (arba) jų kopijų netikslumus, neteisingumą ar neišsamumą, raštu arba elektroninio ryšio priemonėmis per 5 darbo dienas nuo šių aplinkybių paaiškėjimo turi kreiptis į ARSIS duomenų teikėjus ir pareikalauti, kad ši informacija ar duomenys būtų patikslinti, ištaisyti ar papildyti Nuostatų 48 punkte nurodytu būdu. Jei ARSIS duomenų teikėjui nėra suteiktos prieigos teisės pasinaudoti Nuostatų 48 punkte nurodytu būdu, jis privalo ARSIS tvarkytojui raštu ar elektroninio ryšio priemonėmis pateikti patikslintus, ištaisytus ar papildytus duomenis, o ARSIS tvarkytojas įrašo juos į duomenų bazę per 5 darbo dienas nuo patikslintų, papildytų ar ištaisytų duomenų gavimo.

27. ARSIS duomenų gavėjas turi teisę reikalauti ištaisyti netikslius duomenis. Pastebėjęs jam perduotų duomenų netikslumus, jis patikslina juos ARSIS priemonėmis, o jeigu tokios teisės ARSIS tvarkytojas jam nėra suteikęs, raštu arba elektroninio ryšio priemonėmis ne vėliau kaip per 5 darbo dienas apie tai praneša ARSIS tvarkytojui, kartu pateikdamas netikslumus pagrindžiančius dokumentus. ARSIS tvarkytojas privalo per 10 darbo dienų nuo informacijos apie ARSIS duomenų netikslumus ir juos pagrindžiančių dokumentų gavimo patikrinti pateiktą informaciją. Informacijai pasitvirtinus, jis privalo ištaisyti netikslumus ir raštu arba elektroninio ryšio priemonėmis pranešti apie tai ARSIS duomenų gavėjui, o informacijai nepasitvirtinus – raštu arba elektroninio ryšio priemonėmis pranešti ją pateikusiam ARSIS duomenų gavėjui apie atsisakymą ištaisyti netikslumus.

28. ARSIS tvarkytojo atsisakymas teikti duomenis gali būti skundžiamas Lietuvos Respublikos administracinių bylų teisenos įstatymo nustatyta tvarka.

VI SKYRIUS
ARSIS DUOMENŲ SAUGA

29. Už ARSIS duomenų (informacijos) saugą pagal kompetenciją atsako ARSIS valdytojas ir ARSIS tvarkytojas.

30. ARSIS duomenų teikėjai atsako už pateikiamų duomenų vientisumą ir teisingumą, taip pat už prašymų suteikti, pakeisti, sustabdyti ir (ar) panaikinti naudotojo prieigą prie ARSIS savo darbuotojams pateikimą laiku ARSIS tvarkytojui.

31. ARSIS duomenų sauga užtikrinama vadovaujantis:

31.1. Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos duomenų saugos nuostatais, valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos saugos politiką įgyvendinančiais dokumentais, parengtais vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu;

31.2. 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“;

31.3. 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“;

31.4. Lietuvos standartais LST ISO/IEC „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo priemonių praktikos nuostatai“ ir LST ISO/IEC „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“;

31.5. kitais informacinių sistemų ir elektroninės informacijos saugą reguliuojančiais teisės aktais.

32. ARSIS naudotojai jungiasi prie ARSIS naudodamiesi tik ARSIS programine įranga ir saugiu kompiuterių tinklu, užtikrinančiu saugų informacijos perdavimą. ARSIS naudotojui jungiantis prie ARSIS ir dirbant su šia sistema, fiksuojamas jo unikalus identifikatorius, leidžiantis nustatyti asmens tapatybę.

33. Asmens duomenų saugumas užtikrinamas vadovaujantis Bendruoju duomenų apsaugos reglamentu.

34. Asmenys, tvarkantys ARSIS duomenis, informaciją, dokumentus ir jų kopijas, yra įpareigoti saugoti asmens duomenų paslaptį. Ši pareiga galioja ir jiems pasitraukus iš valstybės tarnybos, perėjus dirbti į kitas pareigas, pasibaigus jų darbo ar sutartiniams santykiams.

35. ARSIS valdytojas, ARSIS tvarkytojas ir ARSIS naudotojai teisės aktų nustatyta tvarka atsako už neteisėtą gaunamų iš ARSIS duomenų (informacijos) atskleidimą, naudojimą ar kitokią neteisėtą veiką, susijusią su ARSIS.

36. Duomenų saugojimo ARSIS duomenų bazėje terminai:

36.1. Nuostatų 16.1, 16.3−16.7 ir 16.9 papunkčiuose (išskyrus Nuostatų 36.3 papunktyje nurodytus papunkčius) nurodyti duomenys saugomi 10 metų nuo informacinės sistemos ar registro išregistravimo iš RISR;

36.2. Nuostatų 16.2 papunktyje nurodyti duomenys saugomi 10 metų nuo atitinkamą reikalavimą nustatančio teisės akto pripažinimo netekusiu galios;

36.3. Nuostatų 16.8.2 ir 16.8.3 papunkčiuose nurodyti asmens duomenys yra saugomi 1 metus nuo informacinės sistemos ar registro išregistravimo iš RISR;

36.4. Nuostatų 16.8.1 papunktyje nurodyti asmens duomenys yra saugomi 1 metus nuo naudotojo paskyros uždarymo.

37. Pasibaigus nurodytiems duomenų saugojimo terminams, ARSIS duomenys sunaikinami Lietuvos Respublikos dokumentų ir archyvų įstatymo nustatyta tvarka.

38. Asmens duomenys tvarkomi ir duomenų subjekto teisės įgyvendinamos vadovaujantis Asmens duomenų tvarkymo ir duomenų subjektų teisių įgyvendinimo krašto

apsaugos sistemoje taisyklėmis, patvirtintomis Lietuvos Respublikos krašto apsaugos ministro 2015 m. gruodžio 3 d. įsakymu Nr. V-1253 „Dėl Asmens duomenų tvarkymo ir duomenų subjektų teisių įgyvendinimo krašto apsaugos sistemoje taisyklių patvirtinimo“.

VII SKYRIUS
ARSIS FINANSAVIMAS

39. ARSIS kūrimas, tvarkymas ir priežiūra finansuojami Lietuvos Respublikos valstybės biudžeto lėšomis.

VIII SKYRIUS
ARSIS MODERNIZAVIMAS IR LIKVIDAVIMAS

40. ARSIS modernizuojama ir likviduojama Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo ir Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo nustatyta tvarka.

41. Likviduojamos ARSIS duomenys negali būti sunaikinami, išskyrus Lietuvos Respublikos įstatymuose ar Europos Sąjungos teisės aktuose nustatytus atvejus, ir privalo būti perduoti kitai valstybės informacinei sistemai arba valstybės archyvams Lietuvos Respublikos dokumentų ir archyvų įstatymo nustatyta tvarka.

IX SKYRIUS
BAIGIAMOSIOS NUOSTATOS

42. Informacinės sistemos ar registro valdytojas arba tvarkytojas, jei jam pavedė valdytojas, paskiria už šios informacinės sistemos ar registro duomenų tvarkymą atsakingą asmenį (toliau – atsakingas asmuo). Gali būti skiriami keli atsakingi asmenys, tačiau vienas iš jų turi būti šios informacinės sistemos ar registro saugos įgaliotinis.

43. Dėl prieigos prie ARSIS teisės atsakingam asmeniui suteikimo informacinės sistemos ar registro valdytojas arba tvarkytojas ARSIS tvarkytojui pateikia prašymą registruoti ARSIS naudotoją ir atsakingo asmens užpildytą pasižadėjimą laikytis duomenų saugos reikalavimų, kurių formos nustatytos Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos naudotojų administravimo taisyklėse, patvirtintose Lietuvos Respublikos krašto apsaugos ministro. Prašyme turi būti nurodyta, ar informacinio ištekliaus valdytojas (tvarkytojas) turi teisę naudotis Lietuvos standartais LST ISO/IEC 27001 ir LST ISO/IEC 27002.

44. Informacinės sistemos ar registro valdytojas arba tvarkytojas, jei jam pavedė valdytojas, pateikia prašymą ARSIS tvarkytojui suteikti prieigą prie ARSIS paskirtam saugos įgaliotiniui ne vėliau kaip per 10 (dešimt) darbo dienų nuo saugos įgaliotinio paskyrimo.

45. ARSIS naudotojai administruojami Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos naudotojų administravimo taisyklių nustatyta tvarka.

46. Pateikdamas Nuostatų 48 punkte nurodytus duomenis, atsakingas asmuo juos susieja su Nuostatų 16.10 papunktyje nurodytais ARSIS klasifikatoriais.

47. Nuostatų 48 punkte nurodytus duomenis atsakingas asmuo atnaujina ne vėliau kaip per 5 darbo dienas nuo jų pasikeitimo. Nuostatų 16.5 papunktyje nurodyti duomenys atnaujinami ne vėliau kaip per 5 darbo dienas nuo 16.5.5 papunktyje nurodytos saugos priemonių įgyvendinimo projekto pabaigos datos.

48. Informacinių sistemų ir registrų valdytojai ir (ar) tvarkytojai leidžiamosios kreipties būdu (sąsaja tarp sistemų) ir (arba) ARSIS naudotojai interaktyviai (per interneto naršyklę) į ARSIS pateikia duomenis:

48.1. 16.3 papunktyje nurodytus duomenis – ne vėliau kaip per 5 darbo dienas nuo atitinkamos informacinės sistemos ar registro informacinių technologijų saugos atitikties vertinimo ataskaitos patvirtinimo;

48.2. 16.4−16.5 papunkčiuose nurodytus duomenis – ne vėliau kaip per 5 darbo dienas nuo:

48.2.1. atitinkamos informacinės sistemos ar registro informacinių technologijų saugos atitikties vertinimo metu pastebėtų trūkumų šalinimo plano patvirtinimo;

48.2.2. rizikos įvertinimo ir rizikos valdymo priemonių plano patvirtinimo;

48.3. 16.6 papunktyje nurodytus duomenis – ne vėliau kaip per 5 darbo dienas nuo rizikos įvertinimo ataskaitos patvirtinimo;

48.4. 16.7 papunktyje nurodytus duomenis – ne vėliau kaip per 5 darbo dienas nuo saugumo įvykio užregistravimo;

48.5. 16.8.3 papunktyje nurodytus duomenis – ne vėliau kaip per 5 darbo dienas nuo saugos įgaliotinio paskyrimo.

_____