Suvestinė redakcija nuo 2018-01-10

Nutarimas paskelbtas: Žin. 2013, Nr. 86-4310, i. k. 1131100NUTA00000716

Nauja redakcija nuo 2016-08-19:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

LIETUVOS RESPUBLIKOS VYRIAUSYBĖ

NUTARIMAS 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

2013 m. liepos 24 d. Nr. 716
Vilnius

Vadovaudamasi Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 4 straipsnio 3 ir 4 punktais, 18 straipsnio 3 dalimi, 30 straipsnio 2 ir 3 dalimis ir 43 straipsnio 2 dalimi, Lietuvos Respublikos Vyriausybė n u t a r i a:

Patvirtinti pridedamus:

1. Bendrųjų elektroninės informacijos saugos reikalavimų aprašą.
2. Saugos dokumentų turinio gairių aprašą.
3. Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašą.

Teisingumo ministras,
pavaduojantis Ministrą Pirmininką
ir vidaus reikalų ministrą — Juozas Bernatonis

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2013 m. liepos 24 d. nutarimu Nr. 716

BENDRŲJŲ ELEKTRONINĖS INFORMACIJOS SAUGOS REIKALAVIMŲ APRAŠAS

I. SKYRIUS
BENDROSIOS NUOSTATOS

Pakeistas skyriaus pavadinimas:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

1. Bendrųjų elektroninės informacijos saugos reikalavimų aprašo (toliau – Aprašas) tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti valstybės registrų (kadastrų) (toliau – valstybės registras) ir žinybinių registrų duomenis, dokumentus ir informaciją, valstybės informacinių sistemų ir kitų informacinių sistemų informaciją.

2. Aprašo nuostatos privalomos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 1 straipsnio 3 dalyje nurodytoms institucijoms (toliau – institucijos).

Punkto pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

3. Aprašo nuostatos netaikomos įslaptintos informacijos tvarkymui.

4. Apraše vartojamos sąvokos:

4.1. **Elektroninė informacija** – duomenys, dokumentai ir informacija, tvarkomi valstybės registruose, žinybiniuose registruose, valstybės informacinėse sistemose ir kitose informacinėse sistemose, kurias steigia, kuria ir (arba) tvarko valstybės institucijos, valstybės įstaigos, valstybės įmonės, viešosios įstaigos (toliau – informacinė sistema).

4.2. **Elektroninės informacijos sauga** – elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas.

4.3. **Elektroninės informacijos saugos incidentas** – įvykis ar veiksmas, kurie gali sudaryti neteisėto prisijungimo prie informacinės sistemos galimybę, sutrikdyti ar pakeisti informacinės sistemos veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti.

4.4. **Elektroninės informacijos saugos politika** (toliau – saugos politika) – pagrindiniai elektroninės informacijos saugos užtikrinimo ir valdymo principai, reikalavimai, į kuriuos atsižvelgiant turi būti derinami informacinės sistemos veiklos ir naudojimo procesai, procedūros ir rengiami juos reglamentuojantys dokumentai. Saugos politika išdėstoma informacinės sistemos valdytojo tvirtinamuose Informacinės sistemos duomenų saugos nuostatuose (toliau – Saugos nuostatai).

4.5. **Informacinės sistemos administratorius** (toliau – administratorius) – institucijos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, prižiūrintis informacinę sistemą ir (ar) jos infrastruktūrą, užtikrinantis jos veikimą ir elektroninės informacijos saugą, ar kitas asmuo (asmenų grupė), kuriam (kuriai) Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka perduotos informacinės sistemos ir (ar) jos infrastruktūros priežiūros funkcijos (toliau – paslaugų teikėjas).

4.6. **Informacinės sistemos naudotojas** – institucijos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, ar kitas asmuo, informacinių sistemų veiklą reglamentuojančių teisės aktų nustatyta tvarka pagal kompetenciją naudojantis ir (ar) tvarkantis elektroninę informaciją.

4.7. **Informacinės sistemos saugos įgaliotinis** (toliau – saugos įgaliotinis) – institucijos valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį, koordinuojantis ir prižiūrintis saugos politikos įgyvendinimą informacinėje sistemoje.

4.8. **Konfidencialumas** – elektroninės informacijos savybė – su informacinėje sistemoje tvarkoma elektronine informacija gali susipažinti tik tą daryti įgalioti asmenys.

4.9. **Prieinamumas** – elektroninės informacijos savybė – elektroninė informacija gali būti tvarkoma reikiamu metu.

4.10. **Vientisumas** – elektroninės informacijos savybė – elektroninė informacija nebuvo atsitiktinai ar neteisėtai pakeista ar sunaikinta.

4.11. Kitos Apraše vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme ir Lietuvos standartuose LST ISO/IEC 27001:2013 ir LST ISO/IEC 27002:2014.

Punkto pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

5. Elektroninės informacijos sauga informacinėse sistemose turi atitikti krašto apsaugos ministro tvirtinamus Techninius informacinių sistemų elektroninės informacijos saugos reikalavimus.

Punkto pakeitimai:
Nr. 20, 2018-01-03, paskelbta TAR 2018-01-09, i. k. 2018-00337

II. SKYRIUS
SAUGOS UŽTIKRINIMAS

Pakeistas skyriaus pavadinimas:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

6. Užtikrinant elektroninės informacijos saugą, rekomenduojama vadovautis Lietuvos standartais LST ISO/IEC 27001:2013 ir LST ISO/IEC 27002:2014, taip pat kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo metodai“ grupės standartais, apibūdinančiais saugų elektroninės informacijos tvarkymą.

Punkto pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

7. Informacinės sistemos valdytojas privalo turėti pagal Lietuvos Respublikos Vyriausybės patvirtintą Saugos dokumentų turinio gairių aprašą parengtus, su krašto apsaugos ministro įgaliota institucija, įgyvendinančia valstybės informacinių išteklių saugos politiką, suderintus ir patvirtintus šiuos saugos dokumentus:

Punkto pakeitimai:
Nr. 20, 2018-01-03, paskelbta TAR 2018-01-09, i. k. 2018-00337

7.1. Saugos nuostatus;

7.2. Saugaus elektroninės informacijos tvarkymo taisykles;

7.3. Informacinės sistemos veiklos tęstinumo valdymo planą;

7.4. Informacinės sistemos naudotojų administravimo taisykles.

Punkto pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

8. Aprašo 7.2–7.4 papunkčiuose nurodytus saugos dokumentus (toliau – saugos politiką įgyvendinantys dokumentai) tvirtina informacinės sistemos valdytojas po to, kai patvirtina su krašto apsaugos ministro įgaliota institucija, įgyvendinančia valstybės informacinių išteklių saugos politiką, suderintus Saugos nuostatus. Kai 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“, 5 punkte

nustatytu atveju informacinė sistema steigiama Lietuvos Respublikos Vyriausybės nutarimu, Lietuvos Respublikos Vyriausybė gali priimti ir nutarimą dėl Aprašo 7 punkte nurodytų dokumentų tvirtinimo.

Punkto pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452
Nr. 20, 2018-01-03, paskelbta TAR 2018-01-09, i. k. 2018-00337

9. Krašto apsaugos ministro įgaliotai institucijai, įgyvendinančiai valstybės informacinių išteklių saugos politiką, teikiamus derinti Aprašo 7 punkte nurodytų dokumentų projektus, be rengėjo, turi vizuoti ir informacinės sistemos valdytojo vadovas. Aprašo 8 punkte nurodytu atveju parengtas Lietuvos Respublikos Vyriausybės nutarimo dėl Aprašo 7 punkte nurodytų dokumentų tvirtinimo projektas derinamas Lietuvos Respublikos Vyriausybės darbo reglamento, patvirtinto Lietuvos Respublikos Vyriausybės 1994 m. rugpjūčio 11 d. nutarimu Nr. 728 „Dėl Lietuvos Respublikos Vyriausybės darbo reglamento patvirtinimo“, nustatyta tvarka.

Punkto pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452
Nr. 20, 2018-01-03, paskelbta TAR 2018-01-09, i. k. 2018-00337

10. Krašto apsaugos ministro įgaliota institucija, įgyvendinanti valstybės informacinių išteklių saugos politiką, išvadas, pastabas ir pasiūlymus dėl Aprašo 7 punkte nurodytų dokumentų projektų turi pateikti per 7 darbo dienas, dėl didelės apimties teisės aktų projektų (daugiau kaip 10 puslapių teksto) – per 12 darbo dienų, o dėl pakartotinai pateiktų derinti Aprašo 7 punkte nurodytų dokumentų projektų – per 5 darbo dienas nuo jų gavimo.

Punkto pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452
Nr. 20, 2018-01-03, paskelbta TAR 2018-01-09, i. k. 2018-00337

11. Teisės akte, kuriuo tvirtinami Saugos nuostatai, nurodomi saugos politiką įgyvendinančių dokumentų rengėjai ir dokumentų parengimo terminai. Saugos politiką įgyvendinantys dokumentai turi būti patvirtinti ne vėliau kaip per 6 mėnesius nuo Saugos nuostatų patvirtinimo dienos.

12. Informacinės sistemos valdytojas gali tvirtinti visų ar kelių jo valdomų informacinių sistemų bendrus saugos dokumentus.

Punkto pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

13. Saugos dokumentai institucijoje turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per metus informacinės sistemos valdytojo vadovo nustatyta tvarka. Saugos dokumentai taip pat turi būti persvarstomi (peržiūrimi) po to, kai atliekamas rizikos įvertinimas ar informacinių technologijų saugos atitikties vertinimas arba institucijoje įvyksta esminių organizacinių, sisteminių ar kitokių pokyčių. Keičiami saugos dokumentai derinami su krašto apsaugos ministro įgaliota institucija, įgyvendinančia valstybės informacinių išteklių saugos politiką, Aprašo nustatyta tvarka. Keičiami saugos dokumentai gali būti su krašto apsaugos ministro įgaliota institucija, įgyvendinančia valstybės informacinių išteklių saugos politiką, nederinami tais atvejais, kai atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar saugos politikos nekeičiantys pakeitimai arba taisoma teisės technika.

Punkto pakeitimai:
Nr. 20, 2018-01-03, paskelbta TAR 2018-01-09, i. k. 2018-00337

14. Patvirtinęs Saugos nuostatus ar jų pakeitimus, informacinės sistemos valdytojas Registrų ir valstybės informacinių sistemų registro nuostatų, patvirtintų Lietuvos Respublikos Vyriausybės 2012 m. spalio 16 d. nutarimu Nr. 1263 „Dėl Registrų sąrašo reorganizavimo į Registrų ir valstybės informacinių sistemų registrą ir Registrų ir valstybės informacinių

sistemų registro nuostatų patvirtinimo“, nustatyta tvarka pateikia šiam registrui reikiamus duomenis ar dokumentų kopijas.
Punkto pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

15. Patvirtintų saugos politiką įgyvendinančių dokumentų ir jų pakeitimų kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo jų patvirtinimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemai krašto apsaugos ministro patvirtintų valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.
Punkto pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452
Nr. 20, 2018-01-03, paskelbta TAR 2018-01-09, i. k. 2018-00337

III. SKYRIUS
SAUGOS ORGANIZAVIMAS

Pakeistas skyriaus pavadinimas:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

16. Už elektroninės informacijos saugą pagal kompetenciją atsako informacinės sistemos valdytojas ir informacinės sistemos tvarkytojas (-ai).

17. Informacinės sistemos valdytojas atsako už saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą.

18. Informacinės sistemos tvarkytojas (-ai) atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka.

19. Informacinės sistemos valdytojas teisės aktu, kuriuo tvirtinami Saugos nuostatai, skiria saugos įgaliotinį arba paveda jį paskirti informacinės sistemos tvarkytojui.

20. 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.

21. Saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, tobulinti elektroninės informacijos saugos srities kvalifikaciją, darbe vadovautis Aprašo, kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis, reglamentuojančiomis elektroninės informacijos saugą.
Punkto pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

22. Saugos įgaliotinis, koordinuodamas ir prižiūrėdamas saugos politikos įgyvendinimą informacinėje sistemoje, atlieka šias funkcijas:

22.1. teikia informacinės sistemos valdytojo ar tvarkytojo, jeigu jis paskyrė saugos įgaliotinį, vadovui pasiūlymus dėl:

22.1.1. administratoriaus (administratorių) paskyrimo ir reikalavimų administratoriui (administratoriams) nustatymo;

22.1.2. institucijos informacinių technologijų saugos atitikties vertinimo atlikimo Aprašo 43 punkte nurodytoje metodikoje nustatyta tvarka;

22.2. teikia informacinės sistemos valdytojo vadovui pasiūlymus dėl saugos dokumentų priėmimo, keitimo;

22.3. koordinuoja elektroninės informacijos saugos incidentų, įvykusių informacinėje sistemoje, tyrimą ir bendradarbiauja su kompetentingoms institucijoms, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės;

22.4. teikia administratoriui (administratoriams) ir informacinės sistemos naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;

22.5. organizuoja rizikos įvertinimą;

22.6. atlieka kitas Saugos nuostatuose, kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą, nustatytas ir Aprašo jam priskirtas funkcijas.

Punkto pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

23. Saugos įgaliotinis negali atlikti administratoriaus funkcijų.

24. Saugos įgaliotinis, atlikdamas savo funkcijas, turi teisę pagal savo įgaliojimus duoti privalomus vykdyti nurodymus ir pavedimus ir kitiems informacinės sistemos valdytojo ir tvarkytojo darbuotojams, jeigu tai būtina saugos politikai įgyvendinti.

25. Saugos įgaliotinis periodiškai organizuoja informacinės sistemos naudotojų mokymą elektroninės informacijos saugos klausimais, įvairiais būdais informuoja juos apie elektroninės informacijos saugos problemas. Mokymo ir informavimo būdai pasirenkami atsižvelgiant į informacinės sistemos specifiką. Mokymas planuojamas, organizuojamas ir vykdomas informacinės sistemos valdytojo tvirtinamuose Saugos nuostatuose nustatyta tvarka.

26. Informacinės sistemos valdytojas arba jo įgaliotas informacinės sistemos tvarkytojas turi paskirti administratorių (administratorius). Jeigu administratoriaus funkcijos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka perduotos paslaugos teikėjui, informacinės sistemos valdytojas ar informacinės sistemos tvarkytojas paskiria darbuotoją, kontroliuojantį šio paslaugos teikėjo darbą.

27. Administratorius (administratoriai) atlieka funkcijas, susijusias su informacinės sistemos 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 informacinės sistemos komponentų sąranka, informacinių sistemų pažeidžiamų vietų nustatymu, saugumo reikalavimų atitikties nustatymu ir stebėsena, reagavimu į elektroninės informacijos saugos incidentus, 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.

28. Atlikdamas (-i) informacinės sistemos sąrankos pakeitimus, administratorius (administratoriai) turi laikytis informacinės sistemos valdytojo nustatytos informacinės sistemos pokyčių valdymo tvarkos, nustatytos informacinės sistemos valdytojo tvirtinamose Saugaus elektroninės informacijos tvarkymo taisyklėse.

29. Administratorius (administratoriai) privalo patikrinti (peržiūrėti) informacinės sistemos sąranką ir informacinės sistemos būsenos rodiklius reguliariai, ne rečiau kaip kartą per metus ir (arba) po informacinės sistemos pokyčio.

30. Informacinių sistemų valdytojas, valdantis daugiau kaip dvi informacines sistemas ar informacines sistemas, kurias sudaro ne mažiau kaip du posistemiai ar funkciškai savarankiškos sudedamosios dalys, gali sudaryti elektroninės informacijos saugos darbo grupes, koordinuosiančias saugos politikos įgyvendinimą institucijoje, elektroninės informacijos saugos priemonių ir metodų taikymą institucijoje ir jos valdomose informacinėse

sistemose, analizuosiančias ir koordinuosiančias institucijų informacinėse sistemose įvykusių elektroninės informacijos saugos incidentų tyrimą ir tvarkysiančias saugos dokumentaciją.

31. Saugos įgaliotinis ir administratorius gali būti paskiriami kelioms informacinės sistemos valdytojo valdomoms informacinėms sistemoms, posistemiams, funkciškai savarankiškoms sudedamosioms dalims ar tam tikroms saugos įgaliotinio ir administratoriaus funkcijoms atlikti, tačiau turi būti užtikrintas tinkamas saugos įgaliotinio ir administratoriaus funkcijų atlikimas. Jeigu skiriami saugos įgaliotiniai ir administratoriai atskirai kiekvienai valdomai informacinei sistemai, posistemiui, funkciškai savarankiškoms sudedamosioms dalims ar tam tikroms saugos įgaliotinio ir administratoriaus funkcijoms atlikti, turi būti aiškiai nurodyta, kokiai informacinei sistemai, posistemiui, funkciškai savarankiškoms sudedamosioms dalims ar kurioms saugos įgaliotinio ir administratoriaus funkcijoms atlikti paskiriamas konkretus saugos įgaliotinis ir administratorius, taip pat vienam iš saugos įgaliotinių ir administratorių pavesta koordinuoti šių saugos įgaliotinių ir administratorių veiklą.

IV. SKYRIUS
SAUGOS INCIDENTŲ VALDYMAS

Pakeistas skyriaus pavadinimas:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

32. Informacinės sistemos naudotojai, pastebėję saugos dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai administratoriui, saugos įgaliotiniui arba jeigu valstybės institucijoje įsteigta informacinių technologijų pagalbos tarnyba – šiai tarnybai.

33. Jeigu saugos įgaliotinis nebuvo informuotas apie Aprašo 32 punkte nurodytus pažeidimus, administratorius arba informacinių technologijų pagalbos tarnyba informuoja saugos įgaliotinį apie šiuos pažeidimus. Įtaręs neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeisiančią informacinės sistemos saugą, saugos įgaliotinis apie tai turi pranešti informacinės sistemos valdytojo vadovui ir kompetentingoms institucijoms, tiriančioms elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais.

34. Elektroninės informacijos saugos incidentų, įvykusių informacinėje sistemoje, tyrimo tvarka nustatoma Informacinės sistemos veiklos tęstinumo valdymo plane.

V. SKYRIUS
RIZIKOS ĮVERTINIMAS

Pakeistas skyriaus pavadinimas:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

35. Saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro prie Lietuvos Respublikos krašto apsaugos ministerijos interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja visų informacinių sistemų rizikos įvertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį informacinių sistemų rizikos įvertinimą. Informacinės sistemos valdytojo ar tvarkytojo, jeigu jis paskyrė saugos įgaliotinį, rašytiniu pavedimu informacinių sistemų rizikos įvertinimą gali atlikti pats saugos įgaliotinis.
Punkto pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452
Nr. 20, 2018-01-03, paskelbta TAR 2018-01-09, i. k. 2018-00337

36. Informacinių sistemų rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama informacinės sistemos valdytojo ar tvarkytojo, jeigu jis paskyrė saugos įgaliotinį, vadovui. Rizikos įvertinimo ataskaita rengiama įvertinant rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausieji rizikos veiksniai yra šie:

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

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

36.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

Punkto pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

37. Atsižvelgdamas į rizikos įvertinimo ataskaitą, informacinės sistemos valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

38. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

VI. SKYRIUS
INFORMACINĖS SISTEMOS POKYČIŲ VALDYMAS

Pakeistas skyriaus pavadinimas:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

39. Informacinės sistemos valdytojas užtikrina informacinės sistemos pokyčių (toliau – pokyčiai) valdymo planavimą, apimantį pokyčių identifikavimą, suskirstymą į kategorijas pagal pokyčio tipą (administracinis, organizacinis ar techninis), įtakos vertinimą ir pokyčių prioritetų nustatymo procesus. Su tuo susijusios nuostatos numatomos informacinės sistemos valdytojo tvirtinamose Saugaus elektroninės informacijos tvarkymo taisyklėse ar kitame informacinės sistemos valdytojo patvirtintame teisės akte.

40. Visi pokyčiai, galintys sutrikdyti ar sustabdyti informacinės sistemos darbą, turi būti suderinti su informacinės sistemos valdytojo vadovu ar duomenų valdymo įgaliotiniu ir vykdomi tik gavus jų raštišką pritarimą. Pokyčius turi teisę inicijuoti duomenų valdymo įgaliotinis, saugos įgaliotinis ar administratorius, o įgyvendinti – administratorius.

41. Informacinės sistemos sąrankos aprašai turi būti nuolat atnaujinami ir rodyti esamą informacinės sistemos sąrankos būklę.

42. Pokyčiai, galintys daryti neigiamą įtaką elektroninės informacijos konfidencialumui, vientisumui ar prieinamumui, turi būti patikrinti bandomojoje aplinkoje, kurioje nėra

konfidencialių ir asmens duomenų ir kuri atskirta nuo eksploatuojamos informacinės sistemos.

VII. SKYRIUS
INFORMACINIŲ TECHNOLOGIJŲ SAUGOS ATITIKTIES VERTINIMAS

Pakeistas skyriaus pavadinimas:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

43. Informacinių technologijų saugos atitikties vertinimo metodiką nustato krašto apsaugos ministras.
Punkto pakeitimai:
Nr. 20, 2018-01-03, paskelbta TAR 2018-01-09, i. k. 2018-00337

44. Atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama informacinės sistemos valdytojo ar tvarkytojo, jeigu jis paskyrė saugos įgaliotinį, vadovui, ir pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato informacinės sistemos valdytojo vadovas.

45. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

VIII. SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ ATSAKOMYBĖ

Pakeistas skyriaus pavadinimas:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

46. Tvarkyti informacinės sistemos elektroninę informaciją gali tik informacinės sistemos naudotojai, susipažinę su saugos dokumentais ir sutikę laikytis jų reikalavimų.

47. Informacinės sistemos naudotojų supažindinimą su saugos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą organizuoja saugos įgaliotinis. Supažindinimo būdai pasirenkami atsižvelgiant į informacinės sistemos specifiką, tačiau turi būti užtikrintas susipažinimo įrodomumas.

48. Informacinės sistemos naudotojai, pažeidę Aprašo ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako įstatymų nustatyta tvarka.

49. Informacinės sistemos naudotojai privalo saugoti duomenų ir informacijos paslaptį, įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą.

_____

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2013 m. liepos 24 d. nutarimu Nr. 716

SAUGOS DOKUMENTŲ TURINIO GAIRIŲ APRAŠAS

I. SKYRIUS
BENDROSIOS NUOSTATOS

Pakeistas skyriaus pavadinimas:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

1. Saugos dokumentų turinio gairių apraše (toliau – Aprašas) nustatomas valstybės registro (kadastro), žinybinio registro, valstybės informacinės sistemos ir kitų informacinių sistemų (toliau – informacinė sistema) duomenų saugos nuostatų, Saugaus elektroninės informacijos tvarkymo taisyklių, Informacinės sistemos veiklos tęstinumo valdymo plano ir Informacinės sistemos naudotojų administravimo taisyklių (toliau – saugos dokumentai) turinys.

2. Apraše vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos Vyriausybės patvirtintame Bendrųjų elektroninės informacijos saugos reikalavimų apraše ir Lietuvos standartuose LST ISO/IEC 27001:2013 ir LST ISO/IEC 27002:2014.

Punkto pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

II. SKYRIUS
INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ TURINIO REIKALAVIMAI

Pakeistas skyriaus pavadinimas:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

3. Informacinės sistemos duomenų saugos nuostatus (toliau – saugos nuostatai) sudaro šie skyriai:

3.1. „Bendrosios nuostatos“, kuriame turi būti nurodyta:

3.1.1. elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys ir tikslai;

3.1.2. informacinės sistemos valdytojo ir tvarkytojo (tvarkytojų), kitų subjektų, kuriems taikomi saugos nuostatų reikalavimai, pavadinimai ir adresai (jeigu dėl didelio skaičiaus ar kitų priežasčių neįmanoma išvardyti visų subjektų, būtina nurodyti jų grupes pagal veiklos ar pavaldumo pobūdį);

3.1.3. informacinės sistemos valdytojo ir tvarkytojo (tvarkytojų), informacinės sistemos saugos įgaliotinio (toliau – saugos įgaliotinis), informacinės sistemos administratoriaus (toliau – administratorius) funkcijos (jeigu paskiriami keli saugos įgaliotiniai ar administratoriai, turi būti atskirai nurodytos kiekvieno saugos įgaliotinio ir administratoriaus funkcijos);

3.1.4. teisės aktų, kuriais vadovaujamasi tvarkant elektroninę informaciją ir užtikrinant jos saugumą, sąrašas.

3.2. „Elektroninės informacijos saugos valdymas“, kuriame turi būti nurodyta:

3.2.1. informacinėje sistemoje tvarkomos elektroninės informacijos svarbos kategorija, priskyrimo tam tikrai svarbos kategorijai kriterijai, jeigu informacinėje sistemoje tvarkoma skirtingos svarbos elektroninė informacija – nurodomos visos elektroninės informacijos svarbos kategorijos, priskyrimo tam tikrai svarbos kategorijai kriterijai;

3.2.2. informacinės sistemos kategorija, priskyrimo tam tikrai kategorijai kriterijus;

3.2.3. pagrindinės informacinės sistemos valdytojo nuostatos dėl rizikos veiksnių vertinimo, pagrindinių rizikos vertinimo kriterijų apibūdinimas (rizikos veiksnių vertinimo metodika, naudojami rizikos vertinimo dokumentai (vadovai, brošiūros, klausimynai, rekomendacijos, interaktyvios priemonės (kompiuterinės programos) ir panašiai), vertinimo periodiškumas, vertinimo apimtis ir kita);

3.2.4. elektroninės informacijos saugos priemonių parinkimo principai.

3.3. „Organizaciniai ir techniniai reikalavimai“, kuriame turi būti nurodyta:

3.3.1. programinės įrangos, skirtos apsaugoti informacinę sistemą nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir panašiai), naudojimo nuostatos ir jos atnaujinimo reikalavimai (nurodomas ilgiausias leistinas neatnaujinimo laikas);

3.3.2. programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos;

3.3.3. kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kita) pagrindinės naudojimo nuostatos;

3.3.4. leistinos kompiuterių (ypač nešiojamųjų) naudojimo ribos (jeigu kompiuterius leidžiama naudoti nustatytoms funkcijoms atlikti ne institucijos patalpose, turi būti nurodytos papildomos saugos priemonės, taikytinos tokiems kompiuteriams (šifravimas, papildomas tapatybės patvirtinimas, prisijungimo ribojimai, rakinimo įrenginių naudojimas ir panašiai);

3.3.5. metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą (nurodomas nuotolinio prisijungimo prie informacinės sistemos būdas, protokolas, elektroninės informacijos keitimosi formatai, šifravimo, elektroninės informacijos kopijų skaičiaus reikalavimai, reikalavimas teikti ir (ar) gauti elektroninę informaciją automatiniu būdu tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas ir panašiai);

3.3.6. pagrindiniai atsarginių elektroninės informacijos kopijų darymo ir atkūrimo reikalavimai.

3.4. „Reikalavimai personalui“, kuriame turi būti nurodyta:

3.4.1. informacinės sistemos naudotojų, administratoriaus (administratorių) ir saugos įgaliotinio kvalifikaciniai reikalavimai;

3.4.2. informacinės sistemos naudotojų mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo dažnumo reikalavimai.

3.5. „Informacinės sistemos naudotojų supažindinimo su saugos dokumentais principai“, kuriame turi būti nurodyti supažindinimo ir pakartotinio supažindinimo su saugos dokumentais, kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, ir atsakomybe už saugos dokumentų nuostatų pažeidimus, pagrindiniai reikalavimai, būdai.

3.6. Prireikus ir kitos Lietuvos standartuose LST ISO/IEC 27001:2013 ir LST ISO/IEC 27002:2014 esančios saugaus elektroninės informacijos tvarkymo nuostatos.

Punkto pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

III. SKYRIUS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLIŲ TURINIO REIKALAVIMAI

Pakeistas skyriaus pavadinimas:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

4. Saugaus elektroninės informacijos tvarkymo taisykles sudaro šie skyriai:

4.1. „Bendrosios nuostatos“, kuriame turi būti nurodyta:

4.1.1. informacinėje sistemoje tvarkomos elektroninės informacijos (jos grupių) sąrašas; jeigu visa tvarkoma elektroninė informacija (jos grupės) nurodyta informacinės sistemos

nuostatose, gali būti pateikiamos nuorodos į atitinkamus informacinės sistemos nuostatų punktus; jeigu informacinėje sistemoje tvarkoma skirtingos svarbos elektroninė informacija – nurodoma atitinkama elektroninės informacijos grupė ir jos svarbos kategorija;

4.1.2. už informacinėje sistemoje tvarkomos elektroninės informacijos (jos grupių), priskirtų tam tikrai elektroninės informacijos svarbos kategorijai, tvarkymą atsakingų informacinės sistemos naudotojų ar informacinės sistemos naudotojų grupių sąrašas.

4.2. „Techninių ir kitų saugos priemonių aprašymas“, kuriame turi būti nurodyta:

4.2.1. kompiuterinės įrangos saugos priemonės;

4.2.2. sisteminės ir taikomosios programinės įrangos saugos priemonės;

4.2.3. elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės;

4.2.4. patalpų ir aplinkos saugumo užtikrinimo priemonės (įėjimo kontrolė, elektros tiekimas, aplinkos drėgnumas, darbo vietos temperatūra, priešgaisrinė sauga);

4.2.5. kitos priemonės, naudojamos elektroninės informacijos saugai užtikrinti (pavyzdžiui, informacinės sistemos darbo apskaitos priemonės ir panašiai).

4.3. „Saugus elektroninės informacijos tvarkymas“, kuriame turi būti nurodyta:

4.3.1. saugaus elektroninės informacijos keitimo, atnaujinimo, įvedimo ir naikinimo užtikrinimo tvarka;

4.3.2. informacinės sistemos naudotojų veiksmų registravimo tvarka;

4.3.3. atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarka;

4.3.4. saugaus elektroninės informacijos perkėlimo ir teikimo susijusioms informacinėms sistemoms, elektroninės informacijos gavimo iš jų užtikrinimo tvarka;

4.3.5. elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo nustatymo tvarka;

4.3.6. programinės ir techninės įrangos keitimo ir atnaujinimo tvarka;

4.3.7. informacinės sistemos pokyčių (toliau – pokyčiai) valdymo tvarka, apimanti šiuos procesus:

4.3.7.1. pokyčių identifikavimas;

4.3.7.2. pokyčių suskirstymas į kategorijas, atsižvelgiant į pokyčių svarbą, aktualumą, poreikį ir panašiai;

4.3.7.3. pokyčių įtakos vertinimas;

4.3.7.4. pokyčių prioritetų nustatymas;

4.3.7.5. pokyčių atlikimas;

4.3.8. jeigu pokyčių valdymo tvarka išdėstyta kitame informacinės sistemos valdytojo patvirtintame teisės akte, pateikiama nuoroda į konkretų teisės aktą;

4.3.9. nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių naudojimo tvarka.

4.4. „Reikalavimai, keliami informacinėms sistemoms funkcionuoti reikalingoms paslaugoms ir jų teikėjams“, kuriame turi būti nurodyta:

4.4.1. paslaugų teikėjų prieigos prie informacinės sistemos lygiai ir sąlygos;

4.4.2. reikalavimai, keliami patalpoms, įrangai, informacinių sistemų priežiūrai, elektroninės informacijos perdavimui tinklais ir kitoms paslaugoms.

IV. SKYRIUS
INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANO TURINIO REIKALAVIMAI

Pakeistas skyriaus pavadinimas:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

5. Informacinės sistemos veiklos tęstinumo valdymo planą (toliau – planas) sudaro šie skyriai:

5.1. „Bendrosios nuostatos“, kuriame turi būti nurodyta:

5.1.1. nuostata, kad planas įsigalioja įvykus elektroninės informacijos saugos incidentui;

5.1.2. saugos įgaliotinio, administratoriaus (administratorių), informacinės sistemos naudotojų ir kitų asmenų įgaliojimai ir veiksmai pagal planą, tai yra įvykus elektroninės informacijos saugos incidentui;

5.1.3. nuostata, kad planas privalomas informacinės sistemos tvarkytojams, valdytojui, saugos įgaliotiniui, administratoriui (administratoriams) ir informacinės sistemos naudotojams;

5.1.4. finansinių ir kitokių išteklių, numatomų informacinės sistemos veiklai atkurti įvykus elektroninės informacijos saugos incidentui, šaltiniai;

5.1.5. informacinės sistemos veiklos kriterijai, pagal kuriuos galima nustatyti, ar informacinės sistemos veikla atkurta.

5.2. „Organizacinės nuostatos“, kuriame turi būti nurodyta:

5.2.1. informacinės sistemos veiklos tęstinumo valdymo grupės (toliau – veiklos tęstinumo valdymo grupė) sudėtis (vadovas, pavaduotojas ir kiti nariai);

5.2.2. veiklos tęstinumo valdymo grupės funkcijos:

5.2.2.1. situacijos analizė ir sprendimų informacinės sistemos veiklos tęstinumo valdymo klausimais priėmimas;

5.2.2.2. bendravimas su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;

5.2.2.3. bendravimas su susijusių informacinių sistemų veiklos tęstinumo valdymo grupėmis;

5.2.2.4. bendravimas su teisėsaugos ir kitomis institucijomis, institucijos darbuotojais ir kitomis interesų grupėmis;

5.2.2.5. finansinių ir kitų išteklių, reikalingų informacinės sistemos veiklai atkurti, įvykus elektroninės informacijos saugos incidentui, naudojimo kontrolė;

5.2.2.6. elektroninės informacijos fizinė sauga įvykus elektroninės informacijos saugos incidentui;

5.2.2.7. logistika (žmonių, daiktų, įrangos gabenimas ir jo organizavimas);

5.2.2.8. informacinės sistemos veiklos atkūrimo priežiūra ir koordinavimas;

5.2.2.9. kitos veiklos tęstinumo valdymo grupei pavestos funkcijos;

5.2.3. informacinės sistemos veiklos atkūrimo grupės (toliau – veiklos atkūrimo grupė) sudėtis (vadovas, pavaduotojas ir kiti nariai (nurodomos asmenų, atsakingų už tam tikrų funkcijų atlikimą, ne mažiau kaip 2 kiekvienai funkcijai atlikti, pareigybės); į veiklos atkūrimo grupę neturėtų būti įtraukiami asmenys, įeinantys į veiklos tęstinumo valdymo grupės sudėtį (išskyrus išimtinius atvejus, kai nepakanka žmogiškųjų išteklių veiklos atkūrimo grupei sudaryti);

5.2.4. veiklos atkūrimo grupės funkcijos:

5.2.4.1. tarnybinių stočių veikimo atkūrimo organizavimas;

5.2.4.2. kompiuterių tinklo veikimo atkūrimo organizavimas;

5.2.4.3. informacinės sistemos elektroninės informacijos atkūrimo organizavimas;

5.2.4.4. taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

5.2.4.5. darbo kompiuterių veikimo atkūrimo ir prijungimo prie kompiuterių tinklo organizavimas;

5.2.4.6. kitos veiklos atkūrimo grupei pavestos funkcijos;

5.2.5. informacinės sistemos veiklos atkūrimo detalusis planas, kuriame nurodyti veiksmų vykdymo eiliškumas, terminai, atsakingi vykdytojai; rekomenduojama numatyti atskirus plano scenarijus informacinės sistemos veiklai atkurti po skirtingo pobūdžio ir masto elektroninės informacijos saugos incidentų;

5.2.6. reikalavimai, keliami atsarginėms patalpoms, naudojamoms informacinės sistemos veiklai atkurti įvykus elektroninės informacijos saugos incidentui, atsarginių patalpų adresas ir būdai, kaip iki jų nuvykti;

5.2.7. veiklos tęstinumo valdymo grupės ir veiklos atkūrimo valdymo grupės komunikavimo reikalavimai (dažnumas, formos ir kita).

5.3. „Aprašomosios nuostatos“, kuriame turi būti nurodyta:

5.3.1. parengtų ir saugomų dokumentų sąrašas:

5.3.1.1. dokumentas, kuriame nurodyti informacinių technologijų įrangos parametrai ir už šios įrangos priežiūrą atsakingas (-i) administratorius (administratoriai), minimalus informacinės sistemos veiklai atkurti nesant administratoriaus, kuris dėl komandiruotės, ligos ar kitų priežasčių negali operatyviai atvykti į darbo vietą, reikiamos kompetencijos ar žinių lygis;

5.3.1.2. dokumentas, kuriame nurodyta minimalaus funkcionalumo informacinių technologijų įrangos, tinkamos institucijos poreikius atitinkančiai informacinės sistemos veiklai užtikrinti įvykus elektroninės informacijos saugos incidentui, specifikacija;

5.3.1.3. dokumentas, kuriame nurodyti kiekvieno pastato, kuriame yra informacinės sistemos įranga, aukšto patalpų brėžiniai ir juose pažymėti:

5.3.1.3.1. tarnybinės stotys;

5.3.1.3.2. kompiuterių tinklo ir telefonų tinklo mazgai;

5.3.1.3.3. kompiuterių tinklo ir telefonų tinklo laidų vedimo tarp pastato aukštų vietos;

5.3.1.3.4. elektros įvedimo pastate vietos;

5.3.1.4. dokumentas, kuriame nurodytos kompiuterių tinklo fizinio ir loginio sujungimo schemos;

5.3.1.5. dokumentas, kuriame nurodytos elektroninės informacijos teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutartys, atsakingų už šių sutarčių įgyvendinimo priežiūrą asmenų pareigas;

5.3.1.6. dokumentas, kuriame nurodyta programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos;

5.3.1.7. dokumentas, kuriame nurodytas veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės narių sąrašas su kontaktiniais duomenimis, leidžiančiais pasiekti šiuos asmenis bet kuriuo metu;

5.3.2. už Aprašo 5.3.1 papunktyje nurodytų dokumentų parengimą atsakingo asmens pareigos;

Punkto pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

5.3.3. už Aprašo 5.3.1 papunktyje nurodytų dokumentų saugojimą atsakingas (-i) administratorius (administratoriai);

Punkto pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

5.3.4. kai institucija naudoja (pagal nuomos, panaudos ar kitas sutartis) visą informacinės sistemos techninę įrangą ar jos dalį, priklausančias ir esančias trečiosios šalies patalpose – sutarties su trečiąja šalimi data ir numeris; sutarties kopija turi būti saugoma administratoriaus (administratorių).

5.4. „Plano veiksmingumo išbandymo nuostatos“, kuriame turi būti nurodyta:

5.4.1. plano veiksmingumo paskutinio ir kito planuojamo išbandymo būdas ir periodiškumas;

5.4.2. asmuo, atsakingas už išbandant plano veiksmingumą pastebėtų trūkumų ataskaitos parengimą ir pateikimą informacinės sistemos valdytojui;

5.4.3. išbandant plano veiksmingumą pastebėtų trūkumų šalinimo principai.

V. SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLIŲ TURINIO REIKALAVIMAI

Pakeistas skyriaus pavadinimas:

Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

6. Informacinės sistemos naudotojų administravimo taisykles sudaro šie skyriai:

6.1. „Bendrosios nuostatos“, kuriame turi būti nurodyta:

6.1.1. subjektai, kuriems bus taikomos šios taisyklės;

6.1.2. prieigos prie elektroninės informacijos principai.

6.2. „Informacinės sistemos naudotojų ir administratorių įgaliojimai, teisės ir pareigos“, kuriame turi būti nurodyta:

6.2.1. informacinės sistemos naudotojų įgaliojimai, teisės ir pareigos tvarkant elektroninę informaciją;

6.2.2. informacinės sistemos administratoriaus (administratorių) prieigos prie informacinės sistemos lygiai ir juose taikomi elektroninės informacijos saugos reikalavimai (elektroninės informacijos skaitymas, kūrimas, atnaujinimas, naikinimas, informacinės sistemos naudotojų informacijos, prieigos teisių redagavimas ir panašiai).

6.3. „Saugaus elektroninės informacijos teikimo informacinės sistemos naudotojams kontrolės tvarka“, kuriame turi būti nurodyta:

6.3.1. tvarka, kuria bus registruojami ir išregistruojami informacinės sistemos naudotojai, ir už šių veiksmų atlikimą atsakingas asmuo;

6.3.2. priemonės informacinės sistemos naudotojų tapatybei nustatyti;

6.3.3. informacinės sistemos naudotojų slaptažodžių sudarymo, galiojimo trukmės ir keitimo reikalavimai;

6.3.4. sąlygos ir atvejai, kai panaikinama informacinės sistemos naudotojų teisė dirbti su konkrečia elektronine informacija;

6.3.5. leistini nuotolinio informacinės sistemos naudotojų prisijungimo prie informacinės sistemos būdai.

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2013 m. liepos 24 d. nutarimu Nr. 716
(Lietuvos Respublikos Vyriausybės,
2016 m. rugpjūčio 11 d. nutarimo Nr. 826
redakcija)

ELEKTRONINĖS INFORMACIJOS, SUDARANČIOS VALSTYBĖS INFORMACINIUS IŠTEKLIUS, SVARBOS ĮVERTINIMO IR VALSTYBĖS INFORMACINIŲ SISTEMŲ, REGISTRŲ IR KITŲ INFORMACINIŲ SISTEMŲ KLASIFIKAVIMO GAIRIŲ APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas (toliau – Aprašas) nustato elektroninės informacijos (toliau – informacija), sudarančios valstybės informacinius išteklius, svarbos nustatymo kriterijus, valstybės informacinių sistemų, registrų ir kitų informacinių sistemų (toliau – informacinės sistemos) klasifikavimo pagal informacijos svarbą tvarką.

2. Aprašo nuostatos netaikomos įslaptintos informacijos tvarkymui.

3. Apraše vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos mobilizacijos ir priimančiosios šalies paramos įstatyme, Lietuvos Respublikos Vyriausybės patvirtintame Bendrųjų elektroninės informacijos saugos reikalavimų apraše (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas).

II SKYRIUS
INFORMACIJOS SVARBOS ĮVERTINIMAS

4. Informacijos svarba nustatoma pagal jos konfidencialumo, vientisumo ir (ar) prieinamumo galimo praradimo neigiamą poveikį valstybės ir Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 1 straipsnio 3 dalyje nurodytų institucijų (toliau – institucijos) veiklai.

5. Informacijos konfidencialumo, vientisumo ir (ar) prieinamumo galimo praradimo neigiamas poveikis įvertinamas vadovaujantis šiais kriterijais:

5.1. žalos žmogaus teisėms ir teisėtiems interesams mastas;

5.2. gyvybiškai svarbių valstybės funkcijų, nurodytų Gyvybiškai svarbių valstybės funkcijų sąraše, patvirtintame Lietuvos Respublikos Vyriausybės 2012 m. gegužės 29 d. nutarimu Nr. 631 „Dėl Gyvybiškai svarbių valstybės funkcijų sąrašo patvirtinimo“ (toliau – gyvybiškai svarbios valstybės funkcijos), sutrikdymo mastas: visos valstybės, keliems ministrams ar vienam ministrui pavestų valdymo sričių;

5.3. ekonominės žalos mastas;

5.4. žalos aplinkai mastas;

5.5. grėsmės nacionaliniam saugumui mastas;

5.6. žalos valstybės tarptautiniams įsipareigojimams mastas.

6. Įvertinus informacijos konfidencialumo, vientisumo ir (ar) prieinamumo galimo praradimo neigiamą poveikį, informacija priskiriama vienai iš 4 kategorijų:

6.1. ypatingos svarbos informacija;

6.2. svarbi informacija;

6.3. vidutinės svarbos informacija;

6.4. mažiausios svarbos informacija.

7. Ypatingos svarbos informacijos kategorijai priskiriama informacija, jeigu ji atitinka bent 2 iš šių kriterijų, tai yra jeigu dėl informacijos konfidencialumo, vientisumo ir (ar) prieinamumo praradimo gali kilti grėsmė, kad prasidės procesai, galintys:

7.1. sukelti pavojų žmogaus gyvybei arba kitaip pažeisti daugiau nei pusės valstybės gyventojų kitas teises ir teisėtus interesus;

7.2. lemti, kad nebus atliekama (-os) kuri nors (kurios nors) gyvybiškai svarbi (-ios) valstybės funkcija (-os) visos valstybės mastu;

7.3. padaryti didesnius kaip 3 000 000 eurų finansinius nuostolius vienai ar kelioms institucijoms;

7.4. padaryti žalą aplinkai daugiau nei 5 apskrityse;

7.5. sukelti pavojų valstybės suverenitetui, teritorijos vientisumui ir konstitucinei santvarkai ar viešajam saugumui daugiau nei 5 apskrityse;

7.6. sukelti tarptautinių sutarčių ir įsipareigojimų pažeidimą, kurio padarinių šalinimo nuostoliai būtų didesni kaip 3 000 000 eurų.

8. Svarbios informacijos kategorijai priskiriama informacija, jeigu ji atitinka bent 2 iš šių kriterijų, tai yra jeigu dėl informacijos konfidencialumo, vientisumo ir (ar) prieinamumo praradimo gali kilti grėsmė, kad prasidės procesai, galintys:

8.1. sudaryti sąlygas kilti pavojui žmogaus gyvybei arba sukelti pavojų žmogaus sveikatai ar kitaip pažeisti daugiau kaip 5 procentų, bet ne daugiau nei pusės valstybės gyventojų kitas teises ir teisėtus interesus;

8.2. lemti, kad nebus atliekama (-os) kuri nors (kurios nors) gyvybiškai svarbi (-ios) funkcija (-os) daugiau nei vienam ministrui pavestose valdymo srityse;

8.3. vienai ar kelioms institucijoms padaryti finansinių nuostolių, didesnių nei 300 000 eurų, bet ne didesnių nei 3 000 000 eurų;

8.4. padaryti žalą aplinkai daugiau nei vienoje, bet ne daugiau nei 5 apskrityse;

8.5. sukelti grėsmę viešajam saugumui daugiau nei vienoje, bet ne daugiau nei 5 apskrityse;

8.6. sukelti tarptautinių sutarčių ir įsipareigojimų pažeidimą, kurio padarinių šalinimo nuostoliai būtų didesni nei 300 000 eurų, bet ne didesni nei 3 000 000 eurų.

9. Vidutinės svarbos informacijos kategorijai priskiriama informacija, jeigu ji atitinka bent 2 iš šių kriterijų, tai yra jeigu dėl informacijos konfidencialumo, vientisumo ir (ar) prieinamumo praradimo gali kilti grėsmė, kad prasidės procesai, galintys:

9.1. pažeisti daugiau nei 1 procento, bet ne daugiau nei 5 procentų valstybės gyventojų teises ir teisėtus interesus;

9.2. lemti, kad nebus atliekama (-os) kuri nors (kurios nors) gyvybiškai svarbi (-ios) funkcija (-os) vienam ministrui pavestoje valdymo srityje;

9.3. vienai ar kelioms institucijoms padaryti finansinių nuostolių, didesnių nei 30 000 eurų, bet ne didesnių nei 300 000 eurų;

9.4. padaryti žalą aplinkai daugiau nei vienoje vienos apskrities savivaldybėje;

9.5. sukelti pavojų viešajam saugumui daugiau nei vienoje vienos apskrities savivaldybėje;

9.6. sukelti tarptautinių sutarčių ir įsipareigojimų pažeidimą, kurio padarinių šalinimo nuostoliai būtų didesni nei 30 000 eurų, bet ne didesni nei 300 000 eurų.

10. Mažiausios svarbos informacijos kategorijai priskiriama informacija, kuri nepatenka į Aprašo 6.1–6.3 papunkčiuose nurodytas kategorijas.

11. Finansinės žalos verčių, nurodytų Aprašo 7.3, 7.6, 8.3, 8.6, 9.3, 9.6 papunkčiuose, nustatymo principai:

11.1. įvertinama tiesioginė žala, atsižvelgiant į šiuos aspektus:

11.1.1. galimos tiesioginės informacijos konfidencialumo, vientisumo ir prieinamumo visiško atkūrimo sąnaudos;

11.1.2. nuostoliai ir žala, galimi dėl informacijos konfidencialumo, vientisumo ir prieinamumo praradimo sukeltų neigiamų padarinių trukmės: laikotarpis, kurį veiklos nebūtų galima vykdyti įprastu būdu arba jai vykdyti reikėtų alternatyvių organizacinių priemonių;

11.2. įvertinama netiesioginė žala, atsižvelgiant į šiuos aspektus:

11.2.1. nuostoliai ir žala, kuriuos patirtų tiesiogiai organizaciškai ir technologiškai susiję institucijos ir ūkio subjektai; nustatomas susijusių subjektų kiekis ir galimos žalos kiekvienai subjektų grupei vidutinis dydis, jeigu tokias grupes tikslinga išskirti; suskaičiuotos grupių nuostolių vertės sudedamos;

11.2.2. nuostoliai ir žala, kurią netiesiogiai patirtų kiti subjektai, susiję per tiesiogiai organizaciškai ir technologiškai susijusias institucijas ir ūkio subjektus; nustatomas susijusių subjektų kiekis ir galimos žalos kiekvienai subjektų grupei vidutinis dydis, jeigu tokias grupes tikslinga išskirti atskirai; suskaičiuotos grupių nuostolių vertės sudedamos;

11.3. Aprašo 11.1 ir 11.2 papunkčiuose nurodytos vertės sudedamos.

III SKYRIUS
INFORMACINIŲ SISTEMŲ KLASIFIKAVIMAS PAGAL INFORMACIJOS SVARBĄ

12. Informacinės sistemos pagal jose tvarkomos informacijos svarbą skirstomos į 4 kategorijas (pirmoji – aukščiausioji, ketvirtoji – žemiausioji kategorija):

12.1. pirmajai kategorijai priskiriamos informacinės sistemos, kuriose tvarkoma ypatingos svarbos informacija;

12.2. antrajai kategorijai priskiriamos informacinės sistemos, kuriose tvarkoma svarbi informacija;

12.3. trečiajai kategorijai priskiriamos informacinės sistemos, kuriose tvarkoma vidutinės svarbos informacija;

12.4. ketvirtajai kategorijai priskiriamos informacinės sistemos, kuriose tvarkoma mažiausios svarbos informacija.

IV SKYRIUS
INFORMACIJOS IR INFORMACINĖS SISTEMOS PRISKYRIMAS SVARBOS KATEGORIJAI

13. Informacinėje sistemoje tvarkomos informacijos svarbą vertina šios informacinės sistemos valdytojas, vadovaudamasis Aprašo nuostatomis, ir informacinėje sistemoje tvarkomos informacijos ir informacinės sistemos svarbos kategorijas nurodo rengiamame informacinės sistemos duomenų saugos nuostatų projekte.

14. Informacinės sistemos valdytojas, Bendrųjų elektroninės informacijos saugos reikalavimų apraše nustatyta tvarka teikdamas derinti informacinės sistemos duomenų saugos nuostatų projektą krašto apsaugos ministro įgaliotai institucijai, įgyvendinančiai valstybės informacinių išteklių saugos politiką, lydimuosiuose dokumentuose pagrindžia informacinėje sistemoje tvarkomos informacijos priskyrimą konkrečiai svarbos kategorijai, atsižvelgdamas į konkrečios informacinės sistemos ypatumus, sąsajas su kitomis informacinėmis sistemomis ir jų vartotojų interesais.

Punkto pakeitimai:

Nr. 20, 2018-01-03, paskelbta TAR 2018-01-09, i. k. 2018-00337

15. Krašto apsaugos ministro įgaliota institucija, įgyvendinanti valstybės informacinių išteklių saugos politiką, derindama informacinės sistemos duomenų saugos nuostatų projektą, įvertina informacinės sistemos valdytojo atliktą informacinėje sistemoje tvarkomos informacijos priskyrimo konkrečiai svarbos kategorijai pagrįstumą ir prireikus pateikia savo išvadas. Krašto apsaugos ministro įgaliota institucija, įgyvendinanti valstybės informacinių

išteklių saugos politiką, turi teisę paprašyti papildomos informacijos, pagrindžiančios informacinėje sistemoje tvarkomos informacijos priskyrimą konkrečiai svarbos kategorijai.
Punkto pakeitimai:
Nr. 20, 2018-01-03, paskelbta TAR 2018-01-09, i. k. 2018-00337

16. Su krašto apsaugos ministro įgaliota institucija, įgyvendinančia valstybės informacinių išteklių saugos politiką, suderinus informacinėje sistemoje tvarkomos informacijos priskyrimą konkrečiai svarbos kategorijai, informacinėje sistemoje tvarkomos informacijos ir informacinės sistemos svarbos kategorijos nurodomos informacinės sistemos duomenų saugos nuostatuose.
Punkto pakeitimai:
Nr. 20, 2018-01-03, paskelbta TAR 2018-01-09, i. k. 2018-00337

Priedo pakeitimai:
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452

Pakeitimai:

1.
Lietuvos Respublikos Vyriausybė, Nutarimas
Nr. 826, 2016-08-11, paskelbta TAR 2016-08-18, i. k. 2016-22452
Dėl Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimo Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ pakeitimo

2.
Lietuvos Respublikos Vyriausybė, Nutarimas
Nr. 20, 2018-01-03, paskelbta TAR 2018-01-09, i. k. 2018-00337
Dėl Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimo 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“ pakeitimo