Suvestinė redakcija nuo 2016-04-13 iki 2020-11-25

Įsakymas paskelbtas: Žin. 2007, Nr. 105-4324, i. k. 1072050ISAK001K-289

LIETUVOS RESPUBLIKOS FINANSŲ MINISTRAS

Į S A K Y M A S
DĖL FINANSŲ MINISTERIJOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2007 m. spalio 3 d. Nr. 1K-289
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų, patvirtintų Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 „Dėl duomenų saugos valstybės ir savivaldybių informacinėse sistemose“ (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891), 6 punktu:

1. T v i r t i n u Lietuvos Respublikos finansų ministerijos informacinių sistemų duomenų saugos nuostatus (pridedama).

2. S k i r i u Informacinių technologijų departamento vyr. specialistą Rimą Čiuladą Finansų ministerijos valdomų ir tvarkomų informacinių sistemų saugos įgaliotiniu (toliau – saugos įgaliotinis). Laikinai nesant saugos įgaliotinio dėl ligos, komandiruotės ar kitų objektyvių priežasčių, šias funkcijas laikinai atlieka Informacinių technologijų departamento direktorius.

Punkto pakeitimai:
Nr. 1K-232, 2011-06-30, Žin., 2011, Nr. 81-3995 (2011-07-05), i. k. 1112050ISAK001K-232

3. P a v e d u saugos įgaliotiniui per 4 mėnesius nuo šio įsakymo įsigaliojimo parengti:

3.1. saugaus informacinių sistemų elektroninės informacijos tvarkymo taisyklių projektą;

3.2. informacinių sistemų veiklos tęstinumo valdymo plano projektą;

3.3. informacinių sistemų naudotojų administravimo taisyklių projektą.

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

4.1. Lietuvos Respublikos finansų ministro 2004 m. spalio 26 d. įsakymą Nr. 1K-346 „Dėl Lietuvos Respublikos finansų ministerijos duomenų saugos nuostatų patvirtinimo“;

4.2. Lietuvos Respublikos finansų ministro 2006 m. balandžio 6 d. įsakymo Nr. 1K-152 „Dėl Valstybės biudžeto apskaitos ir mokėjimų sistemos bei šios sistemos duomenų saugos nuostatų patvirtinimo“ (Žin., 2006, Nr. 41-1485) 1.2 ir 2 punktus;

4.3. Lietuvos Respublikos finansų ministro 2006 m. liepos 20 d. įsakymo Nr. 1K-263 „Dėl ES struktūrinių fondų ir ES sanglaudos fondo kompiuterinės informacinės valdymo ir priežiūros sistemos bei šios sistemos duomenų saugos nuostatų patvirtinimo“ 2 punktą.

FINANSŲ MINISTRAS RIMANTAS ŠADŽIUS

PATVIRTINTA
Lietuvos Respublikos finansų ministro
2007 m. spalio 3 d. įsakymu Nr. 1K-289
(Lietuvos Respublikos finansų ministro 2015 m. rugpjūčio 13 d. įsakymo Nr. 1K-265 redakcija)

LIETUVOS RESPUBLIKOS FINANSŲ MINISTERIJOS VALDOMŲ IR (ARBA) TVARKOMŲ INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos finansų ministerijos valdomų ir (arba) tvarkomų informacinių sistemų duomenų saugos nuostatai (toliau – saugos nuostatai) nustato saugos politiką – principus ir reikalavimus, užtikrinančius saugų elektroninės informacijos tvarkymą Lietuvos Respublikos finansų ministerijos (toliau – ministerija) valdomose ir (arba) tvarkomose informacinėse sistemose (išskyrus informacinę sistemą „E. sąskaita“ ir Valstybės turto informacinės paieškos sistemą (toliau – VTIPS), kurių duomenų saugos nuostatai tvirtinami atskirai), jų posistemiuose ir duomenų rinkmenose (toliau – IS) atliekant ministerijai pavestas funkcijas.

Punkto pakeitimai:
Nr. 1K-122, 2016-04-08, paskelbta TAR 2016-04-12, i. k. 2016-08670

2. Saugos nuostatuose vartojamos sąvokos:

2.1. **Elektroninė informacija** – ministerijos valdomose ir (arba) tvarkomose IS arba valstybės ir žinybiniuose registruose saugomi, perduodami ar kitaip elektroniniu būdu apdorojami duomenys, dokumentai ir informacija, padedantys sėkmingai atlikti ministerijos funkcijas.

2.2. **IS administratorius** – ministerijos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį (toliau – darbuotojas), atliekantis IS priežiūrą, registruojantis IS naudotojus, skiriantis jiems registravimosi vardus ir nustatantis prieigos prie IS išteklių teises.

2.3. **IS duomenų gavėjas** – valstybės institucija ar įstaiga, Lietuvos Respublikos teisės aktų nustatyta tvarka gaunanti duomenis savo atliekamoms priežiūros ir kontrolės funkcijoms atlikti. IS duomenų gavėjais gali būti kiti fiziniai ir juridiniai asmenys, Lietuvos Respublikos teisės aktų nustatyta tvarka turintys teisę gauti duomenis ir pateikę prašymus ar sudarę elektroninės informacijos teikimo sutartis, kuriose nurodyti duomenų naudojimo tikslai, sąlygos ir tvarka.

2.4. **IS duomenų teikėjas** – fizinis ar juridinis asmuo, Lietuvos Respublikos teisės aktų nustatyta tvarka teikiantis duomenis IS ir sudaręs elektroninės informacijos teikimo sutartį, kurioje nurodyti duomenų naudojimo tikslai, sąlygos ir tvarka.

2.5. **IS duomenų valdytojas** – ministerijos administracijos padalinio, kurio funkcijoms atlikti reikiamą informaciją apdoroja IS, vadovas.

2.6. **IS infrastruktūros administratorius** – darbuotojas, atliekantis IS infrastruktūros priežiūrą, registruojantis IS infrastruktūros naudotojus, skiriantis jiems registravimosi vardus, nustatantis prieigos prie IS infrastruktūros išteklių teises.

2.7. **IS naudotojas** – ministerijos arba kitos institucijos darbuotojas, turintis teisę naudotis IS ištekliais savo funkcijoms atlikti.

2.8. Kitos šiuose saugos nuostatuose vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos teisės aktuose ir Lietuvos standarte LST ISO/IEC 27002:2013.

3. IS valdytojas atsako už saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą.

Punkto pakeitimai:

Nr. 1K-122, 2016-04-08, paskelbta TAR 2016-04-12, i. k. 2016-08670

4. IS tvarkytojas atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka.

Punkto pakeitimai:

Nr. 1K-122, 2016-04-08, paskelbta TAR 2016-04-12, i. k. 2016-08670

5. IS valdytojas skiria IS saugos įgaliotinį (toliau – saugos įgaliotinis), IS administratorius, IS infrastruktūros administratorius, IS duomenų valdytojus, jei reikia, sudaro elektroninės informacijos saugos darbo grupes

6. Ministerijos elektroninės informacijos saugumo užtikrinimo tikslas – saugiai tvarkyti duomenis ministerijos valdomose ir (arba) tvarkomose IS.

7. Ministerijos elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys – saugus duomenų teikimas, teisėtas ir kokybiškas jų tvarkymas užtikrinant tvarkomų duomenų konfidencialumą, vientisumą ir tinkamo lygio prieinamumą.

8. Ministerijos elektroninės informacijos saugos principai:

8.1. suvokimo – laikantis šio principo siekiama užtikrinti elektroninės informacijos saugą, ugdyti suvokimą apie apsisaugojimo nuo galimos grėsmės elektroninei informacijai priemonių naudojimo būtinybę;

8.2. atsakomybės – kiekvienas IS naudotojas turi suvokti savo atsakomybę ir funkcijas saugant elektroninę informaciją. Elektroninės informacijos saugą ministerijos valdomose ir (arba) tvarkomose IS turi užtikrinti IS valdytojas, o ją įgyvendinti – saugos įgaliotinis;

8.3. reagavimo – laikantis šio principo siekiama laiku aptikti elektroninės informacijos saugos incidentus ir užkirsti jiems kelią, keistis informacija apie grėsmę elektroninei informacijai ir kovos su ja priemones ministerijoje ir tarp valstybės institucijų;

8.4. demokratiškumo – ministerijoje elektroninės informacijos sauga turi būti įgyvendinama ir derinama su esminėmis demokratiškos visuomenės vertybėmis (pvz., laisve skleisti informaciją ir ją gauti);

8.5. rizikos įvertinimo – laikantis šio principo siekiama periodiškai vertinti elektroninės informacijos saugos riziką, kad būtų nustatomas esamas elektroninės informacijos saugos lygis ir parenkamos būtinos elektroninės informacijos saugos priemonės;

8.6. elektroninės informacijos saugos kultūros kėlimo – laikantis šio principo siekiama vykdyti nuolatinius elektroninės informacijos tvarkytojų mokymus elektroninės informacijos saugos klausimais ir taip kelti elektroninės informacijos saugos kultūrą ministerijoje;

8.7. elektroninės informacijos saugos priemonių projektavimo ir diegimo – elektroninės informacijos saugos priemonės turi būti kuriamos kartu su IS. Elektroninės informacijos sauga turi būti pamatinis visų informacinių technologijų (toliau – IT) paslaugų elementas, kuriam būtinas nuolatinis lėšų, neviršijančių pačios elektroninės informacijos vertės, skyrimas.

9. Ministerija (Lukiškių g. 2, Vilnius) yra:

9.1. Valstybės biudžeto, apskaitos ir mokėjimų sistemos (toliau – VBAMS) valdytoja ir tvarkytoja;

9.2. Europos Sąjungos struktūrinių fondų ir Europos Sąjungos sanglaudos fondo kompiuterinės informacinės valdymo ir priežiūros sistemos (toliau – SFMIS) valdytoja ir tvarkytoja;

9.3. Viešojo sektoriaus apskaitos konsolidavimo informacinės sistemos (toliau – VSAKIS) valdytoja ir tvarkytoja;

9.4. Finansų ministerijos finansų valdymo ir apskaitos sistemos (toliau – FVAIS) valdytoja ir tvarkytoja;

9.5. Administracinės informacinės sistemos (toliau – AIS) valdytoja ir tvarkytoja;

9.6. ministerijos vidiniams finansinės informacijos analizės poreikiams sukurtų ir naudojamų IS valdytoja ir tvarkytoja;

9.7. Informacinės sistemos „E. sąskaita“ valdytoja;

9.8. Stebėsenos informacinės sistemos (SIS) tvarkytoja;

9.9. VTIPS valdytoja.

Papildyta punktu:
Nr. 1K-122, 2016-04-08, paskelbta TAR 2016-04-12, i. k. 2016-08670

10. Kiti ministerijos valdomų ir (arba) tvarkomų IS valdytojai ir (arba) tvarkytojai:

10.1. Ministro Pirmininko tarnyba (Gedimino pr. 11, Vilnius) yra SIS valdytoja;

10.2. valstybės įmonė Registrų centras (Vinco Kudirkos g. 18-3, Vilnius) yra IS „E. sąskaita“ tvarkytojas;

10.3. valstybės įmonė Turto bankas (Kęstučio g. 45, Vilnius) yra VTIPS tvarkytojas.

Punkto pakeitimai:
Nr. 1K-122, 2016-04-08, paskelbta TAR 2016-04-12, i. k. 2016-08670

11. Tais atvejais, kai IS valdytoja yra ministerija, o IS tvarkytoja – kita institucija, IS valdytoja turi teisę pavesti IS tvarkytojai parengti ir pateikti IS valdytojai tvirtinti šių saugos nuostatų 12.1, 12.2 ir 12.3 papunkčiuose nurodytų dokumentų projektus.

Punkto pakeitimai:
Nr. 1K-122, 2016-04-08, paskelbta TAR 2016-04-12, i. k. 2016-08670

12. IS valdytojas rengia ir tvirtina šiuos saugos politiką įgyvendinančius dokumentus:

12.1. saugaus IS elektroninės informacijos tvarkymo taisykles;

12.2. IS veiklos tęstinumo valdymo planą;

12.3. IS naudotojų administravimo taisykles.

13. Saugos įgaliotinio funkcijos ir atsakomybė:

13.1. teikia IS valdytojui pasiūlymus dėl:

13.1.1. IS administratorių skyrimo (saugos įgaliotinis negali atlikti IS administratoriaus ar IS infrastruktūros administratoriaus funkcijų);

13.1.2. saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

13.1.3. IS saugos reikalavimų atitikties vertinimo atlikimo;

13.2. koordinuoja elektroninės informacijos saugos incidentų, įvykusių IS, tyrimą (išskyrus atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės);

13.3. duoda IS administratoriui ar IS infrastruktūros administratoriui privalomus vykdyti nurodymus;

13.4. teisės aktų nustatyta tvarka organizuoja IT saugos atitikties ir rizikos vertinimą;

13.5. supažindina IS administratorius ir IS infrastruktūros administratorius su ministerijos duomenų saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, taip pat su atsakomybe už šiuose dokumentuose nustatytų reikalavimų nesilaikymą;

13.6. vykdo kitas ministerijos duomenų saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose, reglamentuojančiuose ministerijos duomenų tvarkymo teisėtumą ir saugos valdymą, priskirtas funkcijas;

13.7. atsako už ministerijos IS duomenų saugos politikos įgyvendinimo organizavimą;

13.8. atsako už ministerijos saugos reikalavimų atitiktį Lietuvos Respublikos teisės aktams.

14. IS duomenų valdytojų funkcijos ir atsakomybė:

14.1. rengia IS kūrimo ir plėtros planus;

14.2. kontroliuoja, kaip kuriamos ir tvarkomos valstybės IS ar jų posistemiai, diegiama programinė įranga;

14.3. kontroliuoja lėšų, skirtų IS, panaudojimą;

14.4. atsako už ministerijos IS duomenų tvarkymo, teikimo ir (arba) gavimo teisėtumą ir saugą.

15. IS administratoriaus funkcijos ir atsakomybė:

15.1. atsako už priskirtos IS veikimą, IS naudotojų registravimą ir registravimosi vardų skyrimą, prieigos prie IS teisių nustatymą;

15.2. įvertina IS naudotojų pasirengimą dirbti su IS;

15.3. rengia pasiūlymus dėl IS kūrimo, palaikymo, priežiūros ir duomenų saugos;

15.4. administruoja IS ar jos komponentus (posistemius, duomenų bazių valdymo sistemas, taikomųjų programų sistemas), rengia ir atnaujina IS sąrankos aprašymo dokumentaciją, nustato IS pažeidžiamas vietas, parenka ir diegia saugos priemones bei užtikrina jų atitiktį saugos nuostatų ir saugos politiką įgyvendinančių dokumentų reikalavimams;

15.5. registruoja elektroninės informacijos saugos incidentus ir informuoja apie juos saugos įgaliotinį, teikia pasiūlymus dėl minėtų incidentų pašalinimo;

15.6. tvarkydami IS elektroninę informaciją neatskleidžia, neperduoda tvarkomos informacijos nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija tiek ministerijoje, tiek už jos ribų;

15.7. jei IS tvarkomi asmens duomenys, saugo asmens duomenų paslaptį;

15.8. neperduoda neįgaliotiems asmenims slaptažodžių, naudotojo tapatybės kodų ar kitos informacijos, leidžiančios naudojantis programinėmis ir techninėmis priemonėmis sužinoti asmens duomenis ar kitą IS tvarkomą elektroninę informaciją, ir nesudaro kitų sąlygų susipažinti su IS tvarkoma elektronine informacija;

15.9. teikia IS valdytojui ir saugos įgaliotiniui pasiūlymus dėl saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

15.10. atlieka kitas šiuose saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose priskirtas funkcijas ir vykdo kitus IS valdytojo ar saugos įgaliotinio nurodymus, susijusius su IS sauga;

15.11. atsako už tinkamą saugos nuostatuose nustatytų funkcijų, susijusių su ministerijos IS priežiūra, vykdymą.

16. IS infrastruktūros administratoriaus funkcijos ir atsakomybė:

16.1. administruoja IS veikimą užtikrinančią techninę ir programinę įrangą, infrastruktūrą bei IT paslaugas, užtikrina IS infrastruktūros veikimą, IT paslaugų teikimą ir jų naudotojų registravimą ir registravimosi vardų skyrimą, prieigos prie IS infrastruktūros išteklių teisių nustatymą;

16.2. administruoja priskirtus IS komponentus (kompiuterių, serverių, operacinių sistemų, ugniasienių, įsilaužimo aptikimo sistemų, duomenų perdavimo tinklų), parengia ir keičia IS komponentų sąrankos aprašymo dokumentaciją, pažeidžiamų vietų nustatymą ir saugos priemonių parinkimą bei jų atitiktį saugos nuostatų ir saugos politiką įgyvendinančių dokumentų reikalavimams;

16.3. pagal kompetenciją rengia pasiūlymus dėl IS kūrimo, palaikymo, priežiūros ir elektroninės informacijos saugos;

16.4. registruoja elektroninės informacijos saugos incidentus ir informuoja apie juos saugos įgaliotinį, teikia pasiūlymus dėl minėtų incidentų pašalinimo;

16.5. neatskleidžia, neperduoda tvarkomos informacijos nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija tiek ministerijoje, tiek už jos ribų;

16.6. jei IS tvarkomi asmens duomenys, saugo asmens duomenų paslaptį;

16.7. neperduoda neįgaliotiems asmenims slaptažodžių, naudotojo tapatybės kodų ar kitos informacijos, leidžiančios naudojantis programinėmis ir techninėmis priemonėmis sužinoti asmens duomenis ar kitą IS tvarkomą elektroninę informaciją, ir nesudaro kitų sąlygų susipažinti su IS tvarkoma elektronine informacija;

16.8. teikia IS valdytojui ir saugos įgaliotiniui pasiūlymus dėl saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

16.9. atlieka kitas šiuose saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose priskirtas funkcijas ir kitus IS valdytojo ar saugos įgaliotinio nurodymus, susijusius su IS sauga;

16.10. atsako už tinkamą saugos nuostatuose nustatytų funkcijų, susijusių su IS priežiūra ir IT paslaugų teikimu, vykdymą.

17. IS naudotojų funkcijos:

17.1. vadovaudamiesi IS valdytojo patvirtintais IS nuostatais, šiais saugos nuostatais, IS duomenų teikimo sutartimis, IS naudojimo instrukcijomis ir pareigybių aprašymais, naudoja ministerijos IS;

17.2. tvarko IS elektroninę informaciją ir naudojasi kitomis ministerijos IS teikiamomis galimybėmis pagal nustatytą funkcijoms atlikti reikalingą IS prieigos teisių lygmenį, kuris apriboja naudojimosi elektronine informacija apimtį;

17.3. tvarko tik tą elektroninę informaciją, kuri IS naudotojui prieinama naudojant konkrečios IS programinę įrangą.

17.4. pagal kompetenciją rengia pasiūlymus dėl IS kūrimo, palaikymo, priežiūros ir elektroninės informacijos saugos;

17.5. tvarkydami IS elektroninę informaciją neatskleidžia, neperduoda tvarkomos informacijos nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija;

17.6. jei IS tvarkomi asmens duomenys, saugo asmens duomenų paslaptį;

17.7. neperduoda neįgaliotiems asmenims slaptažodžių, naudotojo tapatybės kodų ar kitos informacijos, leidžiančios naudojantis programinėmis ir techninėmis priemonėmis sužinoti asmens duomenis ar kitą IS tvarkomą elektroninę informaciją, ir nesudaro kitų sąlygų susipažinti su IS tvarkoma elektronine informacija;

17.8. informuoja saugos įgaliotinį, IS administratorių ar IS infrastruktūros administratorių apie elektroninės informacijos saugos incidentus, IS darbo sutrikimus ir teikia pasiūlymus dėl jų pašalinimo;

17.9. vykdo kitas šiuose saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose priskirtas funkcijas ir kitus IS valdytojo, saugos įgaliotinio ir IS administratoriaus nurodymus, susijusius su IS naudojimu ir IS sauga.

18. Tvarkant IS elektroninę informaciją ir rengiant saugos politiką įgyvendinančius dokumentus, vadovaujamasi:

18.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

18.2. Lietuvos Respublikos kibernetinės saugos įstatymu;

18.3. Lietuvos Respublikos valstybės registrų įstatymu;

18.4. 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

18.5. Saugos dokumentų turinio 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

18.6. Bendraisiais reikalavimais organizacinėms ir techninėms 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 duomenų saugumo priemonėms patvirtinimo“;

18.7. Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

18.8. 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“;

18.9. Europos Sąjungos struktūrinių fondų ir Europos Sąjungos sanglaudos fondo kompiuterinės informacinės valdymo ir priežiūros sistemos nuostatais, patvirtintais Lietuvos Respublikos finansų ministro 2006 m. liepos 20 d. įsakymu Nr. 1K-263 „Dėl Europos Sąjungos struktūrinių fondų ir Europos Sąjungos sanglaudos fondo kompiuterinės informacinės valdymo ir priežiūros sistemos nuostatų patvirtinimo“;

18.10. Valstybės biudžeto apskaitos ir mokėjimų sistemos nuostatais, patvirtintais Lietuvos Respublikos finansų ministro 2014 m. vasario 28 d. įsakymu Nr. 1K-073 „Dėl finansų ministro 2006 m. balandžio 6 d. įsakymo Nr. 1K-152 „Dėl Valstybės biudžeto apskaitos ir mokėjimų sistemos bei šios sistemos duomenų saugos nuostatų patvirtinimo“ pakeitimo“;

18.11. Stebėsenos informacinės sistemos nuostatais, patvirtintais Lietuvos Respublikos Vyriausybės 2011 m. gegužės 4 d. nutarimu Nr. 518 „Dėl Stebėsenos informacinės sistemos nuostatų ir Stebėsenos informacinės sistemos duomenų saugos nuostatų patvirtinimo“;

18.12. Viešojo sektoriaus apskaitos ir ataskaitų konsolidavimo informacinės sistemos nuostatais, patvirtintais Lietuvos Respublikos finansų ministro 2011 m. gegužės 13 d. įsakymu Nr. 1K-182 „Dėl Viešojo sektoriaus apskaitos ir ataskaitų konsolidavimo informacinės sistemos nuostatų patvirtinimo“;

18.13. Informacinės sistemos „E. sąskaita“ nuostatais, patvirtintais Lietuvos Respublikos finansų ministro 2014 m. spalio 31 d. įsakymu Nr. 1K-343 „Dėl finansų ministro 2012 m. rugsėjo 6 d. įsakymo Nr. 1K-297 „Dėl Informacinės sistemos „E. sąskaita“ nuostatų patvirtinimo“ pakeitimo“;

18.14. Lietuvos standartu LST ISO/IEC 27002:2014 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ ir LST ISO/IEC 27001:2013 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“ ir kitais standartais.;

18.15. kitais teisės aktais, kurie reglamentuoja elektroninės informacijos tvarkymo teisėtumą, IS valdytojo veiklą ir elektroninės informacijos saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

19. Ministerijos valdomų ir (arba) tvarkomų IS paskirtis – kaupti, apdoroti ir saugoti ministerijos veiklai vykdyti reikalingus duomenis.

20. Kiekvienos IS objektai išvardijami jos nuostatuose, kuriuos tvirtina IS valdytojas.

21. IS kategorijos ir IS tvarkomos informacijos svarba ministerijoje nustatomos vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“:

21.1. prie pirmosios kategorijos priskiriama VBAMS, kurioje tvarkoma ypatingos svarbos elektroninė informacija;

21.2. prie antrosios kategorijos priskiriamos šios IS: VSAKIS, FVAIS, SFMIS, „E. sąskaita“, VTIPS. VSAKIS, SFMIS tvarkoma ypatingos svarbos elektroninė informacija, o FVAIS, „E. sąskaita“, VTIPS – svarbi elektroninė informacija;

Punkto pakeitimai:
Nr. 1K-122, 2016-04-08, paskelbta TAR 2016-04-12, i. k. 2016-08670

21.3. prie trečiosios kategorijos priskiriama AIS, kurioje tvarkoma žinybinės svarbos elektroninė informacija;

21.4. prie ketvirtosios kategorijos priskiriamos visos kitos ministerijos vidiniams poreikiams sukurtos ir naudojamos IS, kuriose tvarkoma kita elektroninė informacija.

22. IS sauga turi būti įgyvendinama siekiant išsaugoti IS elektroninės informacijos savybes. Pirmiausia turi būti diegiamos priemonės, skirtos išsaugoti toms elektroninės informacijos savybėms, kurių praradimas turėtų didžiausią įtaką IS darbui.

23. Pasirenkant saugos priemones prioritetas teikiamas toms priemonėms, kurių diegimas reikalauja mažiausiai sąnaudų ir duoda didžiausią efektą.

24. Prioritetinis ministerijos IS elektroninės informacijos pateikimo būdas yra IT ir elektroninių ryšių priemonėmis. Siektinas ministerijos pirmosios kategorijos IS elektroninės informacijos pasiekiamumo lygis per metus darbo dienomis darbo laiku – 99 procentai.

25. Saugos įgaliotinis, atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius grupės „Informacijos technologija. Saugumo technika“ standartus, kasmet organizuoja visų IS rizikos vertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį IS rizikos vertinimą. IS valdytojo rašytiniu pavedimu IS rizikos vertinimą gali atlikti pats saugos įgaliotinis, dalyvaujant IS duomenų valdytojams

26. IS rizikos vertinimo rezultatai išdėstomi rizikos vertinimo ataskaitoje. Rizikos vertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai.

27. Svarbiausieji IS rizikos veiksniai nurodyti Bendrųjų elektroninės informacijos saugos reikalavimų apraše.

28. Atsižvelgdamas į rizikos vertinimo ataskaitą, IS valdytojo vadovas prireikus tvirtina IS rizikos vertinimo ataskaitą ir IS rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis IS rizikos valdymo priemonėms įgyvendinti.

29. Teisės aktų nustatyta tvarka atliekant IT saugos atitikties vertinimą, būtina:

29.1. įvertinti saugos nuostatų ir saugos politiką įgyvendinančių dokumentų reikalavimų ir realios informacijos saugos situacijos atitiktį;

29.2. inventorizuoti IS techninę ir programinę įrangą;

29.3. patikrinti ne mažiau kaip 10 procentų atsitiktinai parinktų IS naudotojų kompiuterinių darbo vietų, serverių įdiegtas programas ir jų sąranką;

29.4. patikrinti (įvertinti) IS naudotojams suteiktų teisių ir vykdomų funkcijų atitiktį;

29.5. įvertinti pasirengimą užtikrinti IS veiklos tęstinumą įvykus saugos incidentui.

30. Atlikus IT saugos atitikties vertinimą, rengiamas pastebėtų trūkumų šalinimo planas. Trūkumų šalinimo planą tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato IS valdytojo vadovas.

31. Ministerijos valdomų ir (arba) tvarkomų IS elektroninės informacijos saugos priemonių parinkimo pagrindiniai principai yra šie:

31.1. saugos priemonės diegimo kaina turi atitikti saugomos informacijos vertę;

31.2. likutinė rizika turi būti sumažinta iki priimtino lygio;

31.3. kur galima, būtina įdiegti prevencines informacijos saugos priemones.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

32. Ministerijos valdomų ir (arba) tvarkomų IS duomenų teikėjai ir (arba) gavėjai sudaro su ministerija elektroninės informacijos arba duomenų teikimo sutartį, kurioje turi būti nurodyti:

32.1. duomenų naudojimo tikslai ir sąlygos;

32.2. duomenų teikimo ar gavimo būdai ir laikas;

32.3. duomenų teikimo specifikacijos ir kitos sąlygos.

33. IS naudotojai jungiasi prie IS naudodami tik IS programinę įrangą, naudodamiesi techninėmis ir programinėmis priemonėmis, užtikrinančiomis saugų duomenų perdavimą kompiuterių tinklais. Prie pirmosios ir antrosios kategorijų priskirtų IS serveriai turi būti atskiruose loginiuose kompiuterių tinkluose.

34. IS naudotojų tapatybė nustatoma pagal suteiktą tapatybės kodą ir atitinkamą slaptažodį. Teisės naudotis IS funkcinėmis galimybėmis ir tvarkyti IS duomenis IS naudotojams suteikiamos vadovaujantis rašytiniu IS tvarkytojo arba IS duomenų valdytojo prašymu. Jungiantis prie IS ir dirbant IS, fiksuojamas IS naudotojo tapatybės kodas.

35. Kiekvienas atitinkamos IS tvarkytojas atsako už elektroninės informacijos, kuri jam prieinama naudojant IS, tvarkymo teisėtumą ir tvarkomų duomenų saugą.

36. Ministerijos IS duomenų teikėjai ir (arba) gavėjai už duomenų tvarkymo teisėtumą ir gautų arba teikiamų duomenų saugą atsako teisės aktų nustatyta tvarka.

37. Neaktyvumo dirbant su IS laikas, kuriam pasibaigus IS naudotojų ryšio sesijos automatiškai nutraukiamos, nustatytas Lietuvos Respublikos finansų ministerijos valdomų ir (arba) tvarkomų informacinių sistemų naudotojų administravimo taisyklėse. Automatinis IS sesijos nutraukimas, tapatybės kodo blokavimas taikomi ten, kur tai leidžia naudojamos technologijos.

38. Elektroninės informacijos saugai užtikrinti yra taikomos šios bendrosios programinės įrangos naudojimo nuostatos:

38.1. serveriuose, IS administratorių, IS infrastruktūros administratorių, ministerijos valstybės tarnautojų ar darbuotojų kompiuterinėse darbo vietose turi būti naudojama tik legali ir saugi programinė įranga, kuri yra įtraukta į ministerijoje naudojamos programinės įrangos sąrašus;

38.2. antivirusinės programinės įrangos virusų parašų bazės automatinio atnaujinimo ir kompiuterių operacinių sistemų kritinių pataisų diegimo terminai netaikomi toms kompiuterinėms darbo vietoms, kurios yra laikinai nenaudojamos. Pradėjus naudoti kompiuterines darbo vietas, visos pataisos įdiegiamos per 3 darbo dienas.

39. IS duomenų saugai užtikrinti serveriuose taikomos šios programinės įrangos naudojimo nuostatos:

39.1. operacinių sistemų ir taikomųjų programų sąranka parenkama tokiu būdu, kad būtų užtikrintas didžiausias saugumo lygis, sustabdomi nereikalingi darbui procesai;

39.2. ribojama arba blokuojama prieiga prie operacinės sistemos prievadų;

39.3. programinę įrangą atnaujina ir kontroliuoja IS infrastruktūros administratoriai arba IS administratoriai (pagal atliekamas funkcijas). Paslaugų teikėjai programinę įrangą gali atnaujinti tik dalyvaujant IS infrastruktūros administratoriui arba IS administratoriui.

40. IS infrastruktūros administratorių ir IS administratorių kompiuterinėse darbo vietose taikomos šios programinės įrangos naudojimo nuostatos:

40.1. įdiegiama programinė įranga, skirta apsisaugoti nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.). Antivirusinės sistemos virusų parašų bazė atnaujinama automatiškai. Ilgiausias leistinas neatnaujinimo laikas – 5 darbo dienos. Kompiuterio operacinės sistemos kritinės pataisos diegiamos ne vėliau kaip per 5 darbo dienas nuo jų išleidimo;

40.2. programinę įrangą atnaujina ir kontroliuoja IS infrastruktūros administratoriai ir kompiuterines darbo vietas prižiūrintys ministerijos Informacinių technologijų departamento (toliau – ITD) Informacinių technologijų infrastruktūros skyriaus valstybės tarnautojai ar darbuotojai.

41. Duomenų saugai užtikrinti IS naudotojų, ministerijos valstybės tarnautojų ar darbuotojų darbo vietose taikomos šios programinės įrangos naudojimo nuostatos:

41.1. įdiegta programinė įranga, skirta apsisaugoti nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.). Antivirusinės sistemos virusų parašų bazė atnaujinama automatiškai. Ilgiausias leistinas neatnaujinimo laikas – 5 darbo dienos. Kompiuterio operacinės sistemos kritinės pataisos diegiamos automatiškai. Programinę įrangą atnaujina ir kontroliuoja IS infrastruktūros administratoriai ir

kompiuterines darbo vietas prižiūrintys ITD Informacinių technologijų infrastruktūros skyriaus valstybės tarnautojai ar darbuotojai;

41.2. IS naudotojų paskyros apribotų teisių, kurios neleidžia įdiegti papildomos programinės įrangos ir keisti sistemos, kompiuterio ar programinės įrangos sisteminių nustatymų. Programinę įrangą diegia tik ITD valstybės tarnautojai ar darbuotojai. Kai diegimą turi atlikti kiti asmenys (paslaugų teikėjų specialistai), diegimas gali būti atliekamas tik suderinus su ITD ir prižiūrint ITD valstybės tarnautojams ar darbuotojams.

42. IS serveriai ir administravimui naudojami kompiuteriai negali turėti tiesioginio ryšio su internetu, jei toks ryšys nėra būtinas IS veikimui.

43. Administravimui naudojami kompiuteriai prie elektros tinklo turi būti prijungti naudojant nepertraukiamo maitinimo šaltinius.

44. Už IS veikimą užtikrinančios techninės ir programinės įrangos administravimą ir priežiūrą yra atsakingi ITD valstybės tarnautojai ar darbuotojai, kuriems priskirtos atitinkamos IS infrastruktūros administratoriaus funkcijos.

45. IS infrastruktūros administratorius atsako už IS atsarginių kopijų darymą, tikrinimą, saugojimą ir atkūrimą Rezervinio kopijavimo procedūrų vadove nustatyta tvarka. Rezervinio kopijavimo procedūrų vadovo turinio reikalavimai nustatyti Finansų ministerijos valdomų ir (arba) tvarkomų informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse, patvirtintose Lietuvos Respublikos finansų ministro 2008 m. rugpjūčio 8 d. įsakymu Nr. 1K-244 „Dėl Lietuvos Respublikos finansų ministerijos informacinių sistemų naudotojų administravimo taisyklių ir Informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklių patvirtinimo“.

46. Nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių saugojimo, išdavimo ir naudojimo tvarka reglamentuota Finansų ministerijos nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių saugojimo, išdavimo ir naudojimo taisyklėse, patvirtintose Lietuvos Respublikos finansų ministerijos kanclerio potvarkiu.

47. Ministerijoje taikomos šios nešiojamųjų kompiuterių ir juose esančios informacijos apsaugos priemonės:

47.1. turi būti naudojama programinė įranga, leidžianti išsaugoti naudotojo duomenis ir operacinės sistemos atkūrimo kopiją atskiruose naudotojui nematomuose standžiojo disko skirsniuose, tam skirtose optinėse laikmenose ar tam skirtoje tinklo srityje;

47.2. kompiuteris ir (arba) išplėtimo įrenginys turi būti prirakinami specialiu tam skirtu lynu;

47.3. turi būti naudojami šie slaptažodžiai – įjungimo slaptažodis, naudotojo slaptažodis ir administravimo slaptažodis;

47.4. turi būti įdiegta standžiojo disko duomenų apsauga nuo perskaitymo kitame kompiuteryje;

47.5. turi būti TPM1.2 arba 2.0 standartus atitinkanti arba analogiška duomenų apsaugos mikroschema;

47.6. kaip papildoma duomenų saugos priemonė (naudojant kompiuterį už ministerijos ribų) gali būti naudojama programinė įranga, skirta standžiojo disko duomenims koduoti.

48. Naudojant nešiojamuosius kompiuterius ne ministerijos patalpose, draudžiama jungtis prie nežinomų ar nepatikimų bevielių kompiuterių tinklų, naršyti pavojingose ar nepatikimose interneto svetainėse.

49. Jungiantis prie ministerijos vidinio tinklo išteklių nuotoliniu būdu, turi būti naudojamas šifruotas prisijungimas ir papildomos tapatybės patvirtinimo priemonės. Prisijungimo teisė suteikiama tik gavus darbuotojo prašymą ir administracijos padalinio vadovo prašymą.

50. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių ir kitos) pagrindinės naudojimo nuostatos:

50.1. kompiuterių tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienes, ir kitas tinklo apsaugos priemones;

50.2. kompiuterių tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroninį paštą ir IS naudotojų kompiuterių įrangą nuo kenksmingo kodo;

50.3. turi būti naudojama duomenų srautų analizės ir kontrolės įranga, padedanti nustatyti galimų informacijos saugos incidentų priežastis, taip pat naudojama saugos incidentų prevencijai.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

51. Saugos įgaliotinis privalo išmanyti informacijos saugos užtikrinimo principus, savo darbe vadovautis Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugos reikalavimais ir Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų duomenų tvarkymą, standartais ir kitais dokumentais, turėti atitinkamą kvalifikaciją, sugebėti prižiūrėti, kaip įgyvendinama saugos politika, taip pat turėti administravimo, darbo su duomenų bazėmis, operacinėmis sistemomis, taikomosiomis programomis patirties.

52. IS administratorius privalo išmanyti elektroninės informacijos saugos principus, administruoti ir prižiūrėti duomenų bazes ir priskirtas IS, taip pat mokėti užtikrinti jų saugumą, turi būti susipažinęs su šiais saugos nuostatais ir kitais saugos politiką įgyvendinančiais dokumentais.

53. IS infrastruktūros administratorius privalo išmanyti elektroninės informacijos saugos principus, administruoti ir prižiūrėti IS komponentus (kompiuterius, serverius, operacines sistemas, taikomųjų programų sistemas, ugniasienes, įsilaužimo aptikimo sistemas, duomenų perdavimo tinklus), taip pat mokėti užtikrinti jų saugumą, turi būti susipažinęs su šiais saugos nuostatais ir kitais saugos politiką įgyvendinančiais dokumentais.

54. IS naudotojai privalo:

54.1. išklausyti pradinį saugaus darbo su duomenimis mokymą arba susipažinti su šio mokymo medžiaga;

54.2. mokėti dirbti su „Windows“ operacine sistema, biuro taikomosiomis programomis;

54.3. mokėti tvarkyti IS elektroninę informaciją atitinkamos IS naudojimo instrukcijos ir IS nuostatų nustatyta tvarka ir būti susipažinę su šiais saugos nuostatais ir kitais saugos politiką įgyvendinančiais dokumentais.

55. IS naudotojai, pastebėję elektroninės informacijos saugos pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias elektroninės informacijos saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti IS administratoriui ir (arba) saugos įgaliotiniui.

56. Įvykus elektroninės informacijos saugos incidentui, nenumatytai situacijai, saugos įgaliotinio, IS administratoriaus, IS infrastruktūros administratoriaus, IS tvarkytojų ir IS naudotojų veiksmus reglamentuoja Lietuvos Respublikos finansų ministerijos informacinių sistemų veiklos tęstinumo valdymo planas, patvirtintas Lietuvos Respublikos finansų ministro 2012 m. vasario 9 d. įsakymu Nr. 1K-052 „Dėl Lietuvos Respublikos finansų ministerijos valdomų ir (arba) tvarkomų informacinių sistemų veiklos tęstinumo valdymo plano patvirtinimo“.

57. Saugos įgaliotinis ar jo paskirtas ITD valstybės tarnautojas ar darbuotojas kasmet organizuoja IS administratorių, IS infrastruktūros administratorių, IS tvarkytojų ir kitų IS naudotojų mokymus duomenų saugos klausimais, nuolat jiems primena elektroninės informacijos saugos reikalavimus (elektroniniu paštu, per interneto svetainę, atmintinėmis naujai priimtiems ministerijos valstybės tarnautojams ar darbuotojams ir pan.).

58. IS valdytojas užtikrina tinkamą saugos įgaliotinio, IS administratorių, IS infrastruktūros administratorių ir IS naudotojų kvalifikacijos tobulinimą.

V SKYRIUS
IS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

59. IS elektroninę informaciją gali tvarkyti tik IS naudotojai, kurie yra susipažinę su šiais saugos nuostatais, kitais saugos politiką įgyvendinančiais dokumentais, atsakomybe už saugos dokumentų nuostatų pažeidimus ir raštu arba elektroninėmis priemonėmis patvirtinę sutikimą laikytis jų reikalavimų.

60. IS duomenų teikėjai ar gavėjai šių saugos nuostatų ir kitų saugos politiką įgyvendinančių dokumentų kopijas gauna sutarties dėl elektroninės informacijos arba duomenų teikimo pasirašymo metu, jei minėti dokumentai nėra paskelbti IS valdytojo. Kitais atvejais sutartyje pateikiama nuoroda į IS valdytojo tinklalapį.

61. Šie saugos nuostatai ir kiti elektroninės informacijos saugos reglamentavimo dokumentai skelbiami IS valdytojo tinklalapyje.

62. Už IS naudotojų supažindinimą su šiais saugos nuostatais ir kitais saugos politiką įgyvendinančiais dokumentais atsako saugos įgaliotinis.

63. Pakartotinai su saugos dokumentais IS naudotojai supažindinami tik iš esmės pasikeitus IS arba elektroninės informacijos saugą reglamentuojantiems teisės aktams.

64. IS naudotojai, IS infrastruktūros administratoriai, IS administratoriai ir saugos įgaliotinis, pažeidę šių saugos nuostatų ir kitų saugos politiką įgyvendinančių dokumentų nuostatas, atsako teisės aktų nustatyta tvarka.

Priedo pakeitimai:
Nr. 1K-265, 2015-08-13, paskelbta TAR 2016-02-04, i. k. 2016-02273

Pakeitimai:

1.
Lietuvos Respublikos finansų ministerija, Įsakymas
Nr. 1K-232, 2011-06-30, Žin., 2011, Nr. 81-3995 (2011-07-05), i. k. 1112050ISAK001K-232
Dėl finansų ministro 2007 m. spalio 3 d. įsakymo Nr. 1K-289 "Dėl Finansų ministerijos informacinių sistemų duomenų saugos nuostatų patvirtinimo" pakeitimo

2.
Lietuvos Respublikos finansų ministerija, Įsakymas
Nr. 1K-093, 2012-03-09, Žin., 2012, Nr. 32-1502 (2012-03-15), i. k. 1122050ISAK001K-093
Dėl finansų ministro 2007 m. spalio 3 d. įsakymo Nr. 1K-289 "Dėl Finansų ministerijos informacinių sistemų duomenų saugos nuostatų patvirtinimo" pakeitimo

3.
Lietuvos Respublikos finansų ministerija, Įsakymas
Nr. 1K-362, 2012-10-29, Žin., 2012, Nr. 128-6438 (2012-11-06), i. k. 1122050ISAK001K-362
Dėl finansų ministro 2007 m. spalio 3 d. įsakymo Nr. 1K-289 "Dėl Finansų ministerijos informacinių sistemų duomenų saugos nuostatų patvirtinimo" pakeitimo

4.
Lietuvos Respublikos finansų ministerija, Įsakymas
Nr. 1K-265, 2015-08-13, paskelbta TAR 2016-02-04, i. k. 2016-02273
Dėl finansų ministro 2007 m. spalio 3 d. įsakymo Nr. 1K-289 „Dėl Finansų ministerijos informacinių sistemų duomenų saugos nuostatų patvirtinimo“ pakeitimo

5.
Lietuvos Respublikos finansų ministerija, Įsakymas
Nr. 1K-122, 2016-04-08, paskelbta TAR 2016-04-12, i. k. 2016-08670
Dėl finansų ministro 2007 m. spalio 3 d. įsakymo Nr. 1K-289 „Dėl Finansų ministerijos informacinių sistemų duomenų saugos nuostatų patvirtinimo“ pakeitimo