Suvestinė redakcija nuo 2011-07-06 iki 2012-03-15

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 MINISTERIJOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos finansų ministerijos informacinių sistemų duomenų saugos nuostatai (toliau – saugos nuostatai) nustato principus ir reikalavimus, užtikrinančius saugų elektroninės informacijos tvarkymą (toliau – saugos politika) Lietuvos Respublikos finansų ministerijos (toliau – ministerija) valdomose informacinėse sistemose, jų posistemiuose ir duomenų rinkmenose (toliau – IS) atliekant ministerijai pavestas funkcijas.

2. Saugos nuostatuose vartojamos sąvokos:

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

Elektroninė informacija – neįslaptinta informacija (arba duomenys), saugoma, perduodama ar kitaip apdorojama elektroniniu būdu ministerijos valdomose IS, leidžiančiose tokią informaciją saugoti, perduoti ar kitaip apdoroti, arba valstybės ir žinybiniuose registruose ir sudaranti sąlygas sėkmingai atlikti ministerijos funkcijas.

IS administratorius – ministerijos valstybės tarnautojas ar darbuotojas, atliekantis IS priežiūrą, registruojantis IS naudotojus, skiriantis jiems registravimosi vardus, nustatantis prieigos prie IS išteklių teises.

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

IS duomenų teikėjas – valstybės institucija ar įstaiga, taip pat kitas fizinis ar juridinis asmuo, Lietuvos Respublikos teisės aktų nustatyta tvarka turintis teikti duomenis IS ir sudaręs elektroninės informacijos (arba duomenų) teikimo sutartį, kurioje nurodyti duomenų naudojimo tikslai, sąlygos ir tvarka.

IS duomenų valdytojas – ministerijos administracijos padalinio, kurio funkcijoms atlikti reikiamą informaciją apdoroja IS, vadovas. IS duomenų valdytojas, vadovaudamasis IS valdytojo patvirtinta informacinių technologijų strategija, rengia IS kūrimo ir plėtros planus, prižiūri IS kūrimą, diegimą ir tvarkymą, kontroliuoja lėšų, skiriamų IS, panaudojimą.

IS naudotojas – valstybės tarnautojas ar darbuotojas, turintis teisę naudotis IS ištekliais numatytoms funkcijoms atlikti.

Kitos šiuose saugos nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos teisės aktuose bei Lietuvos standartuose LST ISO/IEC 17799: 2006 ir LST ISO/IEC 27001: 2006 vartojamas sąvokas.

3. Už ministerijos valdomų IS elektroninės informacijos tvarkymo teisėtumą ir elektroninės informacijos saugą atsako IS valdytojas – ministerija.

4. IS valdytojas užtikrina valdomų IS elektroninės informacijos saugumą, vientisumą, konfidencialumą, prieinamumą, tinkamą kompiuterių bei komunikacinės įrangos funkcionavimą ministerijoje ir valdomų IS duomenų teikimą IS duomenų gavėjams.

5. IS valdytojas, vadovaudamasis saugos nuostatais, skiria IS saugos įgaliotinį (toliau – saugos įgaliotinis), IS administratorius, administratorius, IS duomenų valdytojus, esant poreikiui

sudaro elektroninės informacijos saugos darbo grupes.

6. Ministerijos elektroninės informacijos saugumo užtikrinimo tikslas – saugiai tvarkyti duomenis ministerijos valdomose 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 principas. Siekiant užtikrinti elektroninės informacijos saugą, ugdyti suvokimą apie apsisaugojimo priemonių nuo galimos grėsmės elektroninei informacijai naudojimo būtinybę.

8.2. Atsakomybės principas. Kiekvienas IS naudotojas turi suvokti savo atsakomybę ir funkcijas saugant elektroninę informaciją. Elektroninės informacijos saugą ministerijos valdomose IS turi užtikrinti IS valdytojo vadovas arba jo įgaliotas asmuo, o ją įgyvendinti – saugos įgaliotinis.

8.3. Reagavimo principas. 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 principas. 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 principas. Periodiškai vertinti elektroninės informacijos saugos riziką, siekiant nustatyti esamą elektroninės informacijos saugos lygį, ir parinkti būtinas elektroninės informacijos saugos priemones.

8.6. Elektroninės informacijos saugos kultūros kėlimo principas. 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 principas. Elektroninės informacijos saugos priemonės turi būti kuriamos kartu su IS. Elektroninės informacijos sauga turi būti pamatinis visų informacinių technologijų (toliau – IT) paslaugų elementas, kuriam būtina užtikrinti nuolatinį lėšų, neviršijančių pačios elektroninės informacijos vertės, skyrimą.

9. Ministerija taip pat yra ir valdomų IS tvarkytojas. Valstybės biudžeto, apskaitos ir mokėjimų sistemos (toliau – VBAMS) tvarkytojais taip pat yra įstaigos ir kiti subjektai, pagal kurių pateiktas mokėjimo paraiškas, vadovaujantis Valstybės biudžeto lėšų išdavimo iš valstybės iždo sąskaitos taisyklėmis, patvirtintomis Lietuvos Respublikos finansų ministro 2000 m. liepos 21 d. įsakymu Nr. 195 (Žin., 2000, Nr. 65-1976, 2004, Nr. 17-513), iš valstybės iždo sąskaitos pervedamos lėšos, skirtos asignavimų valdytojų ir jiems pavaldžių biudžetinių įstaigų ir kitų subjektų programų sąmatoms vykdyti. Europos Sąjungos struktūrinių fondų ir Europos Sąjungos sanglaudos fondo kompiuterinės informacinės valdymo ir priežiūros sistemos (toliau – SFMIS) tvarkytojais taip pat yra valstybės institucijos ir įstaigos, kurios Lietuvos Respublikos Vyriausybės 2001 m. gegužės 31 d. nutarimu Nr. 649 „Dėl institucijų, atsakingų už Europos Sąjungos struktūrinių fondų lėšų, skirtų Lietuvos 2004–2006 metų bendrojo programavimo dokumentui įgyvendinti, administravimą, atsakomybės ir funkcijų paskirstymo“ (Žin., 2001, Nr. 48-1676; 2005, Nr. 51-1700) ir Lietuvos Respublikos Vyriausybės 2001 m. rugpjūčio 24 d. nutarimu Nr. 1026 „Dėl Europos Sąjungos sanglaudos fondo lėšų administravimo Lietuvoje“ (Žin., 2001, Nr. 74-2596; 2004, Nr. 103-3777) įpareigotos administruoti Europos Sąjungos (toliau vadinama – ES) struktūrinių fondų lėšas, skirtas bendrojo programavimo dokumentui įgyvendinti, ir ES sanglaudos fondo lėšas.

10. Kiekvienas IS tvarkytojas tvarko tik tą elektroninę informaciją, kuri jo valstybės tarnautojams ar darbuotojams – IS naudotojams – prieinama naudojant konkrečios IS programinę įrangą.

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

11.1. saugaus IS elektroninės informacijos tvarkymo taisykles;

11.2. IS veiklos tęstinumo valdymo planą;

11.3. IS naudotojų administravimo taisykles.

12. Saugos įgaliotinis organizuoja ir kontroliuoja šių saugos nuostatų įgyvendinimą ir atlieka šias funkcijas:

12.1. teikia IS valdytojui pasiūlymus dėl:

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

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

12.1.3. IS saugos reikalavimų atitikties vertinimo atlikimo;

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

12.3. duoda administratoriams privalomus vykdyti nurodymus;

12.4. teisės aktų nustatyta tvarka atlieka IT saugos atitikties vertinimą. Jei vertinimui atlikti būtina įsigyti vertinimo paslaugas, teikia IS valdytojui pasiūlymus dėl minėtų paslaugų įsigijimo;

12.5. atlieka kitas IS valdytojo vadovo ar jo įgalioto asmens pavestas ir šiais saugos nuostatais jam priskirtas funkcijas.

13. IS duomenų valdytojų funkcijos ir atsakomybė:

13.1. rengia IS kūrimo ir plėtros planus;

13.2. prižiūri IS kūrimą, diegimą ir tvarkymą;

13.3. kontroliuoja lėšų, skirtų IS, panaudojimą.

14. IS administratoriaus funkcijos ir atsakomybė:

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

14.2. įvertina IS naudotojų pasirengimą dirbti su IS;

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

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

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

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

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

14.8. neperduoda neįgaliotiems asmenimis 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;

14.9. 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. Administratoriaus funkcijos ir atsakomybė:

15.1. atsako už IS funkcionavimą užtikrinančios techninės ir programinės įrangos, infrastruktūros bei IT paslaugų administravimą, funkcionavimo užtikrinimą ir jų naudotojų registravimą ir registravimosi vardų skyrimą, prieigos prie IS infrastruktūros išteklių teisių nustatymą;

15.2. atsako už priskirtų IS komponentų (kompiuterių, tarnybinių stočių, operacinių sistemų, ugniasienių, įsilaužimų aptikimo sistemų, duomenų perdavimo tinklų) administravimą, IS komponentų sąrankos aprašymo dokumentacijos parengimą ir atnaujinimą, pažeidžiamų vietų nustatymą ir saugos priemonių parinkimą bei jų atitiktį saugos nuostatų ir saugos politiką įgyvendinančių dokumentų reikalavimams;

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

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

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

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

15.7. neperduoda neįgaliotiems asmenimis 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;

15.8. 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. IS naudotojų funkcijos ir atsakomybė:

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

16.2. 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;

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

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

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

16.6. neperduoda neįgaliotiems asmenimis 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;

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

16.8. 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.

17. Tvarkant IS elektroninę informaciją bei rengiant saugos politiką įgyvendinančius dokumentus, vadovaujamasi:

17.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (Žin., 1996, Nr. 63-1479; 2003, Nr. 15-597);

17.2. Lietuvos Respublikos valstybės registrų įstatymu (Žin., 1996, Nr. 86-2043; 2004, Nr. 124-4488);

17.3. Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, patvirtintais Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891);

17.4. Saugos dokumentų turinio gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070);

17.5. Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymu Nr. 1V-247 (Žin., 2007, Nr. 78-3160);

17.6. Valstybės institucijų ir įstaigų IS klasifikavimo pagal jose tvarkomą elektroninę informaciją gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymu Nr. 1V-247 (Žin., 2007, Nr. 78-3160);

17.7. 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;

17.8. Valstybės biudžeto apskaitos ir mokėjimų sistemos nuostatais, patvirtintais Lietuvos Respublikos finansų ministro 2006 m. balandžio 6 d. įsakymu Nr. 1K-152 (Žin., 2006, Nr. 41-1485);

17.9. Lietuvos standartais LST ISO/IEC 17799: 2006, LST ISO/IEC 27001: 2006, taip pat kitais Lietuvos ir tarptautiniais grupės „Informacijos technologija. Saugumo metodai“ standartais;

17.10. kitais teisės aktais, kuriais reglamentuojamas elektroninės informacijos tvarkymo teisėtumas, IS valdytojo veikla ir elektroninės informacijos saugos valdymas.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

18. Ministerijos valdomų IS paskirtis – kaupti, apdoroti ir saugoti ministerijos veiklai vykdyti reikalingus duomenis.

19. Atitinkamos IS objektai išvardijami jos nuostatuose, kuriuos tvirtina IS valdytojas.

20. Ministerijoje IS kategorijos priskiriamos vadovaujantis Valstybės institucijų ir įstaigų IS klasifikavimo pagal jose tvarkomą elektroninę informaciją gairėmis:

20.1. prie pirmosios kategorijos priskiriamos šios IS: VBAMS ir SFMIS;

20.2. prie trečiosios kategorijos priskiriamos šios IS: Administracinė informacinė sistema, valstybės biudžeto planavimo, kontrolės ir apskaitos programos, valstybės biudžeto skiriamų lėšų kontrolės ir apskaitos programos, valstybės biudžeto ir valstybės piniginių fondų apskaitos, finansinės atskaitomybės ataskaitų formavimo programos (sukurta ir naudojama vidiniams poreikiams);

20.3. prie ketvirtosios kategorijos priskiriamos visos kitos ministerijos vidiniams poreikiams sukurtos ir naudojamos IS.

21. 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.

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

23. Prioritetinis ministerijos IS elektroninės informacijos (arba duomenų) pateikimo būdas yra informacinių technologijų ir elektroninių ryšių priemonės. Siektinas ministerijos elektroninės informacijos pasiekiamumo lygis darbo dienomis darbo laiku – 98 procentai.

24. Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius grupės „Informacijos technologija. Saugumo technika“ standartus ir naudodamas CRAMM (angl. CCTA Risk Analysis and Management Methodology) metodiką, 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.

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

26. Svarbiausieji IS rizikos veiksniai yra išdėstyti Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų 31 punkte.

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

28. Teisės aktų nustatyta tvarka atliekant informacinių technologijų saugos atitikties vertinimą, būtina:

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

28.2. inventorizuoti IS techninę ir programinę įrangą;

28.3. patikrinti ne mažiau kaip 10 procentų atsitiktinai parinktų IS naudotojų kompiuterinių darbo vietų, visose tarnybinėse stotyse įdiegtas programas ir jų sąranką;

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

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

29. Atlikus šių 28 punkte nurodytą vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato IS valdytojo vadovas.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

30. Ministerijos valdomų IS duomenų teikėjai ir/arba gavėjai sudaro su ministerija elektroninės informacijos arba duomenų teikimo sutartį, kurioje turi būti nurodyti:

30.1. duomenų naudojimo tikslai ir sąlygos;

30.2. duomenų teikimo ar gavimo būdai ir laikas;

30.3. teikimo specifikacijos ir kitos sąlygos.

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

32. IS naudotojų tapatybė nustatoma pagal suteiktą tapatybės kodą ir atitinkamą slaptažodį. Teisės naudoti IS funkcinėmis galimybėmis ir tvarkyti IS duomenis jiems suteikiamos vadovaujantis raštišku IS tvarkytojo arba IS duomenų valdytojo prašymu. Jungiantis prie IS ir dirbant, fiksuojamas IS naudotojo tapatybės kodas.

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

34. Ministerijos IS duomenų teikėjai ir/arba gavėjai už duomenų tvarkymo teisėtumą ir gautų arba teikiamų duomenų saugą atsako įstatymų nustatyta tvarka.

35. Ilgiausias neaktyvumo laikas, kuriam pasibaigus IS naudotojų ryšio sesijos yra automatiškai nutraukiamos, yra 30 min. IS naudotojų prieigos teisės yra blokuojamos, jei suteiktas tapatybės kodas yra nenaudojamas 45 dienas. Automatinis IS sesijos nutraukimas, tapatybės kodo blokavimas taikomi ten, kur tai leidžia naudojamos technologijos.

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

36.1. tarnybinėse stotyse, IS administratorių, 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;

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

37. IS duomenų saugai užtikrinti tarnybinėse stotyse taikomos šios programinės įrangos naudojimo nuostatos:

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

37.2. ribojama arba blokuojama prieiga prie operacinės sistemos prievadų;

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

38. Administratorių ir IS administratorių kompiuterinėse darbo vietose taikomos šios programinės įrangos naudojimo nuostatos:

38.1. 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 – penkios darbo dienos. Kompiuterio operacinės sistemos kritinės pataisos diegiamos ne vėliau kaip per 5 darbo dienas nuo jų išleidimo;

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

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

39.1. 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 – penkios darbo dienos. Kompiuterio operacinės sistemos kritinės pataisos diegiamos automatiškai. Programinę įrangą atnaujina ir kontroliuoja administratoriai bei kompiuterines darbo vietas prižiūrintys ITD Informacinių technologijų infrastruktūros skyriaus valstybės tarnautojai ar darbuotojai;

39.2. IS naudotojų paskyros turi būti apribotų teisių, kurios neleidžia įdiegti papildomos programinės įrangos bei 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.

40. IS tarnybinės stotys ir administravimui naudojami kompiuteriai negali turėti tiesioginio ryšio su internetu (nepertraukiamos sesijos), jei toks ryšys nėra būtinas IS funkcionuoti.

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

42. Administratorius atsako už IS atsarginių kopijų darymą ir saugojimą Rezervinio kopijavimo procedūrų vadove nustatyta tvarka. Reikalavimai Rezervinio kopijavimo procedūrų vadovo turiniui nustatyti saugaus IS elektroninės informacijos tvarkymo taisyklėse, kurias tvirtina IS valdytojas.

43. Nešiojamųjų kompiuterių saugojimo, išdavimo ir naudojimo tvarką reglamentuoja Finansų ministerijos nešiojamųjų kompiuterių saugojimo, išdavimo ir naudojimo taisyklės, patvirtintos Lietuvos Respublikos finansų ministerijos valstybės sekretoriaus 2005 m. vasario 4 d. potvarkiu Nr. 2K-004.

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

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

44.2. kompiuteris ir siūlomas išplėtimo įrenginys turi būti prirakinami specialiu tam skirtu lynu;

44.3. turi būti naudojami šie slaptažodžiai – įjungimo slaptažodis, administravimo slaptažodis;

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

44.5. turi būti inventoriaus numeris (Ownership Tag) arba panašus;

44.6. turi būti TPM 1.2 standartus atitinkanti duomenų apsaugos mikroschema arba panaši;

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

IV. REIKALAVIMAI PERSONALUI

45. 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 (Žin., 2004, Nr. 80-2855), 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 darbo su duomenų bazėmis, operacinėmis sistemomis, taikomosiomis programomis patirties.

46. 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.

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

48. IS duomenų tvarkytojai privalo:

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

48.2. mokėti dirbti su „Windows“ operacine sistema, biuro taikomosiomis programomis arba turėti Europos kompiuterio naudotojo pažymėjimą;

48.3. 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.

49. IS tvarkytojai ar IS naudotojai, pastebėję elektroninės informacijos saugos pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias elektroninės informacijos saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti saugos įgaliotiniui ir/arba IS administratoriui.

50. Esant elektroninės informacijos saugos incidentui, nenumatytai situacijai, saugos įgaliotinio, IS administratoriaus, administratoriaus, IS tvarkytojų, IS naudotojų veiksmus reglamentuoja IS veiklos tęstinumo valdymo planas, kurį tvirtina IS valdytojas.

51. Saugos įgaliotinis ar jo paskirtas ITD valstybės tarnautojas ar darbuotojas organizuoja IS administratorių, 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.).

52. IS valdytojas užtikrina tinkamą saugos įgaliotinio, IS administratorių, administratorių, IS naudotojų kvalifikacijos tobulinimą.

V. IS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

53. IS elektroninę informaciją gali tvarkyti tik IS naudotojai, kurie yra susipažinę su šiais saugos nuostatais ir kitais saugos politiką įgyvendinančiais dokumentais ir raštiškai sutikę laikytis jų reikalavimų.

54. 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 nuorodą į IS valdytojo tinklalapį.

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

56. Už IS naudotojų supažindinimą su šiais saugos nuostatais ir kitais saugos politiką įgyvendinančiais dokumentais atsako atitinkamos IS administratorius.

57. IS naudotojai, pažeidę šių saugos nuostatų ir kitų saugos politiką įgyvendinančių

dokumentų nuostatas, atsako teisės aktų nustatyta tvarka.

_____

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