

**Nutarimas netenka galios 2013-08-08:**

*Lietuvos Respublikos Vyriausybė, Nutarimas*

Nr. [716](#), 2013-07-24, Žin., 2013, Nr. 86-4310 (2013-08-07), i. k. 1131100NUTA00000716

*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*

**Suvestinė redakcija nuo 2011-05-11 iki 2013-08-07**

Nutarimas paskelbtas: Žin. 1997, Nr. [83-2075](#), i. k. 0971100NUTA00000952

**Nauja redakcija nuo 2007-06-30:**

Nr. [410](#), 2007-04-25, Žin. 2007, Nr. 49-1891 (2007-05-05), i. k. 1071100NUTA00000410

**LIETUVOS RESPUBLIKOS VYRIAUSYBĖ**

**N U T A R I M A S**

**DĖL ELEKTRONINĖS INFORMACIJOS SAUGOS VALSTYBĖS INSTITUCIJŲ IR  
ĮSTAIGŲ INFORMACINĖSE SISTEMOSE**

1997 m. rugsėjo 4 d. Nr. 952  
Vilnius

Siekdama užtikrinti, kad informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, kokio nors kitokio neteisėto jos tvarkymo, vadovaudamasi Lietuvos Respublikos valstybės registrų įstatymu (Žin., 1996, Nr. [86-2043](#); 2004, Nr. 124-4488), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (Žin., 1996, Nr. [63-1479](#); 2003, Nr. [15-597](#)), įgyvendindama Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinės strategijos iki 2008 metų įgyvendinimo priemonių plano, patvirtinto Lietuvos Respublikos Vyriausybės 2006 m. birželio 19 d. nutarimu Nr. 601 (Žin., 2006, Nr. [70-2575](#)), 2.1 punktą ir atsižvelgdama į tai, kad informacinės sistemos nuolat tobulinamos, Lietuvos Respublikos Vyriausybė n u t a r i a:

Patvirtinti Bendruosius elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimus (pridedama).

MINISTRAS PIRMININKAS

GEDIMINAS VAGNORIUS

SUSISIEKIMO MINISTRAS,  
PAVADUOJANTIS RYŠIŲ IR INFORMATIKOS MINISTRĄ

ALGIS ŽVALIAUSKAS

## **BENDRIEJI ELEKTRONINĖS INFORMACIJOS SAUGOS VALSTYBĖS INSTITUCIJŲ IR ĮSTAIGŲ INFORMACINĖSE SISTEMOSE REIKALAVIMAI**

### **I. BENDROSIOS NUOSTATOS**

1. Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų (toliau vadinama – šie Reikalavimai) tikslas – sudaryti sąlygas saugiai automatinio būdu tvarkyti elektroninę informaciją (toliau vadinama – informacija) valstybės informacinėse sistemose ir valstybės ar žinybiniuose registruose arba kitose informacinėse sistemose (toliau vadinama – informacinė sistema).

2. Šie Reikalavimai privalomi ministerijoms, Vyriausybės įstaigoms, įstaigoms prie ministerijų ir kitoms Lietuvos Respublikos Vyriausybei atskaitingoms valstybės institucijoms ir įstaigoms (toliau vadinama – valstybės institucija).

Techninius informacinių sistemų elektroninės informacijos saugos reikalavimus nustato vidaus reikalų ministras.

*Punkto pakeitimai:*

Nr. [743](#), 2008-07-16, *Žin.*, 2008, Nr. 85-3393 (2008-07-26), i. k. 1081100NUTA00000743

3. Šie Reikalavimai netaikomi įslaptintos informacijos tvarkymui automatinio būdu, išskyrus riboto naudojimo informaciją.

### **II. PAGRINDINĖS SĄVOKOS**

4. Šiuose Reikalavimuose vartojamos sąvokos:

**Saugos politika** – pagrindiniai taikytini informacijos saugos užtikrinimo ir valdymo principai, pagrindinės taisyklės, į kuriuos atsižvelgiant turi būti derinami informacinės sistemos (ar informacinių sistemų) veiklos ir naudojimo procesai, procedūros ir rengiami juos reglamentuojantys dokumentai. Informacijos saugos politika išdėstoma informacinės sistemos valdytojo tvirtinamuose Informacinės sistemos duomenų saugos nuostatuose (toliau vadinama – Nuostatai).

**Saugos įgaliotinis** – valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį, įgyvendinantis elektroninės informacijos saugą informacinėje sistemoje.

**Informacinės sistemos naudotojas** – valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, turintis teisę naudotis informacinės sistemos ištekliais numatytoms funkcijoms atlikti.

**Administratorius** – valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, atliekantis informacinės sistemos priežiūrą.

**Duomenų perdavimas tinklais** – tokia informacinės sistemos funkcija, kai siekiant užtikrinti duomenų tvarkymą, apdorojimą ir teikimą šios sistemos naudotojams, jos dalims ir kitoms informacinėms sistemoms sudaromos sąlygos gauti duomenis ryšių linijomis.

Kitos šiuose Reikalavimuose vartojamos sąvokos atitinka sąvokas, nustatytas Lietuvos Respublikos įstatymuose, kituose teisės aktuose ir Lietuvos standartuose LST ISO/IEC 17799:2006 ir LST ISO/IEC 27001:2006.

*Punkto pakeitimai:*

Nr. [743](#), 2008-07-16, *Žin.*, 2008, Nr. 85-3393 (2008-07-26), i. k. 1081100NUTA00000743

### **III. SAUGOS UŽTIKRINIMAS**

5. Užtikrinant informacijos saugą, rekomenduojama vadovautis Lietuvos standartais LST ISO/IEC 17799:2006, LST ISO/IEC 27001:2006, taip pat kitais Lietuvos ir tarptautiniais

„Informacijos technologija. Saugumo metodai“ grupės standartais, apibūdinančiais saugų informacinės sistemos duomenų tvarkymą.

6. Informacinės sistemos valdytojas privalo turėti pagal Vidaus reikalų ministerijos tvirtinamas Saugos dokumentų turinio gaires parengtus, su Vidaus reikalų ministerija suderintus ir patvirtintus šiuos saugos dokumentus:

- 6.1. Nuostatus;
- 6.2. Saugaus elektroninės informacijos tvarkymo taisykles;
- 6.3. Informacinės sistemos veiklos tęstinumo valdymo planą;
- 6.4. Informacinės sistemos naudotojų administravimo taisykles.

7. Šių Reikalavimų 6.2–6.4 punktuose nurodytus dokumentus (toliau vadinama – saugos politiką įgyvendinantys dokumentai) tvirtina informacinės sistemos valdytojas po to, kai patvirtina su Vidaus reikalų ministerija suderintus nuostatus. Išimtiniais atvejais, kai informacinė sistema steigama kelių pavaldumu nesusijusių valstybės institucijų, sprendimą dėl šių Reikalavimų 6.1–6.4 punktuose nurodytų dokumentų tvirtinimo gali priimti Lietuvos Respublikos Vyriausybė. Šiuo atveju Lietuvos Respublikos Vyriausybė sprendime gali nustatyti kitokias, nenustatytas šiuose Reikalavimuose, informacinės sistemos valdytojo ir tvarkytojo pareigas, susijusias su tvarkos aprašų, taisyklių ir planų, nurodytų šių Reikalavimų 21, 24, 32, 33 ir 39 punktuose, rengimu ir tvirtinimu.

*Punkto pakeitimai:*

Nr. [519](#), 2011-05-04, *Žin.*, 2011, Nr. 55-2642 (2011-05-10), i. k. 1111100NUTA00000519

8. Teisės aktu, kuriuo tvirtinami Nuostatai, skiriamas saugos įgaliotinis arba pavedama informacinės sistemos tvarkytojui paskirti saugos įgaliotinį ir nurodomi saugos politiką įgyvendinančių dokumentų rengėjai bei saugos politiką įgyvendinančių dokumentų patvirtinimo terminai.

*Punkto pakeitimai:*

Nr. [743](#), 2008-07-16, *Žin.*, 2008, Nr. 85-3393 (2008-07-26), i. k. 1081100NUTA00000743

9. Informacinės sistemos valdytojo tvirtinamuose Nuostatuose nustatoma:

- 9.1. informacijos saugumo tikslai, svarba ir esama būklė;
- 9.2. informacijos saugumo užtikrinimo prioritetinės kryptys;
- 9.3. informacinės sistemos ir šioje sistemoje tvarkomų duomenų (toliau vadinama – duomenys) svarba ir pagrindiniai informacinei sistemai, jos dalims ir funkcijoms keliami saugos reikalavimai, pagal kuriuos bus parenkamos atitinkamos saugos priemonės;
- 9.4. saugaus duomenų tvarkymo reikalavimai, kurie apima:
  - 9.4.1. teisės aktų, kuriais vadovaujamosi tvarkant duomenis ir užtikrinant jų saugumą, sąrašą;
  - 9.4.2. informacinės sistemos valdytojo personalo kvalifikacinius reikalavimus;
  - 9.4.3. pagrindines informacinės sistemos valdytojo nuostatas dėl rizikos veiksnių vertinimo, pagrindinių rizikos vertinimo kriterijų apibūdinimą;
- 9.5. informacinės sistemos naudotojų supažindinimo su saugos dokumentais principai;
- 9.6. atsakomybė už saugos dokumentų reikalavimų pažeidimus;
- 9.7. kiti reikalavimai.

10. Saugaus elektroninės informacijos tvarkymo taisyklėse pateikiama:

- 10.1. informacinėje sistemoje esančios informacijos kategorijų sąrašas ir kiekvienai kategorijai priskirtini duomenys;
- 10.2. techninių ir kitų saugos priemonių aprašymas, apimantis kompiuterinės įrangos, sisteminės ir taikomosios programinės įrangos, duomenų perdavimo tinklais saugumo užtikrinimo, patalpų ir aplinkos (įėjimo kontrolė, elektros tiekimas, aplinkos drėgnumas, darbo vietos temperatūra, priešgaisrinė sauga), informacinės sistemos darbo apskaitos ir kitas priemones informacijos saugai užtikrinti;

10.3. informacinės sistemos saugą užtikrinantys reikalavimai, keliami nuomojamų ar perkamų informacinių sistemų funkcionavimui reikalingoms paslaugoms (patalpos, įrangos ir sistemų priežiūra, duomenų perdavimas tinklais ir kitos paslaugos);

10.4. informacinės sistemos ir duomenų vientisumo pažeidimų fiksavimo ir pažeistų duomenų atkūrimo tvarka (naudotojų veiksmų registravimas, atsarginės duomenų kopijos, jų saugojimas, saugojimo kontrolė ir kita);

10.5. saugaus duomenų perkėlimo ar perdavimo tvarka, Nuostatų įgyvendinimo kontrolės tvarka;

10.6. duomenų perdavimo tinklais reikalavimai;

10.7. kiti reikalavimai.

11. Informacinės sistemos veiklos tęstinumo valdymo planui keliami šie reikalavimai:

11.1. Informacinės sistemos veiklos tęstinumo valdymo plane turi būti nurodyta saugos įgaliotinio, administratorių, informacinės sistemos naudotojų funkcijos, įgaliojimai ir veiksmai atkuriant informacinių sistemų veiklą, informacijos saugos incidentų, įvykusių informacinėje sistemoje, tyrimo tvarka.

*Punkto pakeitimai:*

Nr. [743](#), 2008-07-16, Žin., 2008, Nr. 85-3393 (2008-07-26), i. k. 1081100NUTA00000743

11.2. Informacinės sistemos veiklos tęstinumo valdymo plano nuostatos turi būti pagrįstos tam tikrais principais. Privalomi šie pagrindiniai principai:

11.2.1. informacinės sistemos naudotojų gyvybės ir sveikatos apsauga (būtina užtikrinti visų informacinės sistemos naudotojų gyvybės ir sveikatos apsaugą ir saugumą, kol trunka nenumatyta situacija ir likviduojami avarijų padariniai);

11.2.2. informacinės sistemos veiklos atkūrimas (informacinių sistemų veikla atkurama pagal šiame plane numatytą informacinių sistemų funkcijų prioritetą);

11.2.3. informacinės sistemos naudotojų mokymas (informacinės sistemos naudotojai turi būti supažindinti su minėtu planu ir teisės aktais, nustatančiais kiekvieno informacinės sistemos naudotojo atsakomybę);

11.2.4. reguliarius šio plano veiksmingumo išbandymas (plano veiksmingumas turi būti reguliariai išbandomas praktinio mokymo metu; plano veiksmingumo išbandymas gali būti planinis arba neplaninis; atsižvelgiant į gautus rezultatus, šis planas turi būti atitinkamai tikslinamas).

11.3. Informacinės sistemos veiklos tęstinumo valdymo plano nuostatos, be to, gali būti pagrįstos nenumatytų situacijų ir likviduojamų avarijų padarinių valdymo, valstybės institucijos veiklos atkūrimo ir kitais principais.

*Punkto pakeitimai:*

Nr. [743](#), 2008-07-16, Žin., 2008, Nr. 85-3393 (2008-07-26), i. k. 1081100NUTA00000743

12. Informacinės sistemos naudotojų administravimo taisyklėse nustatoma:

12.1. prieinamumo prie duomenų principai;

12.2. informacinės sistemos naudotojų supažindinimo su saugos dokumentais tvarka;

12.3. saugaus duomenų teikimo informacinės sistemos naudotojams kontrolės tvarka (informacinės sistemos naudotojų registravimas, teisės dirbti su informacinės sistemos duomenimis suteikimas, informacinės sistemos naudotojų išregistravimas, informacinės sistemos naudotojų tapatybės nustatymas, specialios informacinės sistemos naudotojų tapatybės nustatymo priemonės, elektroninis parašas ir kita);

12.4. informacinės sistemos naudotojų, turinčių priėjimą prie informacinės sistemos ar atskirų jos komponentų, įgaliojimai, teisės ir pareigos;

12.5. kiti reikalavimai.

13. Informacinių sistemų valdytojams rekomenduojama duomenis teikti naudojant Saugų valstybinį duomenų perdavimo tinklą.

#### IV. SAUGOS ORGANIZAVIMAS

14. Už informacijos tvarkymo teisėtumą ir informacijos saugą atsako informacinės sistemos valdytojas.

15. Informacinės sistemos valdytojas ar tvarkytojas, jeigu jam buvo pavesta skiria saugos įgaliotinį, kuris įgyvendina informacijos saugą informacinėje sistemoje ir atsako už saugos dokumentų reikalavimų vykdymą.

*Punkto pakeitimai:*

Nr. [743](#), 2008-07-16, Žin., 2008, Nr. 85-3393 (2008-07-26), i. k. 1081100NUTA00000743

16. Saugos įgaliotinis privalo išmanyti informacijos saugos užtikrinimo principus, savo darbe vadovautis šiais Reikalavimais, Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta 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.

17. Saugos įgaliotinis, įgyvendindamas elektroninės informacijos saugą informacinėje sistemoje, atlieka šias funkcijas:

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

*Punkto pakeitimai:*

Nr. [743](#), 2008-07-16, Žin., 2008, Nr. 85-3393 (2008-07-26), i. k. 1081100NUTA00000743

17.1.1. administratorių paskyrimo (saugos įgaliotinis negali atlikti administratoriaus funkcijų);

17.1.2. saugos dokumentų priėmimo, keitimo ar panaikinimo;

17.1.3. įstaigos informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

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

17.3. teikia administratoriams privalomus vykdyti nurodymus ir pavedimus;

17.4. atlieka kitas informacinės sistemos valdytojo ar tvarkytojo, jeigu jis paskyrė saugos įgaliotinį vadovo pavestas ir šiais Reikalavimais jam priskirtas funkcijas.

*Punkto pakeitimai:*

Nr. [743](#), 2008-07-16, Žin., 2008, Nr. 85-3393 (2008-07-26), i. k. 1081100NUTA00000743

18. Saugos įgaliotinis periodiškai inicijuoja informacinės sistemos naudotojų mokymą informacijos saugos klausimais, įvairiais būdais informuoja juos apie informacijos saugos problematiką (priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės priimtiems naujiems darbuotojams ir panašiai).

19. Administratoriumi gali būti skiriamas valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, išmanantis darbą su kompiuterių tinklais ir mokantis užtikrinti jų saugumą. Administratorius privalo būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais.

20. Administratorius atlieka funkcijas, susijusias su informacinės sistemos naudotojų pasirengimo dirbti su informacinėmis sistemomis įvertinimu, jų teisėmis, informacinę sistemą sudarančiais komponentais (kompiuteriais, operacinėmis sistemomis, duomenų bazių valdymo sistemomis, taikomųjų programų sistemomis, ugniasienėmis, įsilaužimų aptikimo sistemomis, duomenų perdavimu tinklais), šių informacinę sistemą sudarančių komponentų sąranka, informacinių sistemų pažeidžiamų vietų nustatymu, saugumo reikalavimų atitikties nustatymu.

21. Atlikdami informacinės sistemos funkcijų pakeitimus, administratoriai turi laikytis informacinės sistemos valdytojo nustatytos informacinės sistemos pokyčių valdymo tvarkos.

22. Administratorius turi teisę patikrinti (peržiūrėti) informacinės sistemos sąranką ir informacinės sistemos būsenos rodiklius.

23. Informacinės sistemos naudotojai privalo turėti darbo kompiuteriu įgūdžių.

24. Informacinių sistemų valdytojas, valdantis informacines sistemas, kurias sudaro ne mažiau kaip du posistemiai, gali sudaryti informacijos saugos darbo grupes, koordinuosiančias saugos politikos įgyvendinimą valstybės institucijoje, informacijos saugos priemonių ir metodų taikymą valstybės institucijoje ir jos valdomose informacinėse sistemose, analizuosiančias ir

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

25. Informacinių sistemų valdytojas, valdantis kelias informacines sistemas, taip pat informacines sistemas, kurias sudaro ne mažiau kaip du posistemiai, gali tvirtinti visų valdomų informacinių sistemų bendrus saugos dokumentus ir paskirti visoms valdomoms informacinėms sistemoms vieną saugos įgaliotinį. Skirdamas saugos įgaliotinius kiekvienai valdomai informacinei sistemai, informacinės sistemos valdytojas privalo pavesti vienam iš saugos įgaliotinių koordinuoti saugos įgaliotinių veiklą.

26. Saugos dokumentai valstybės institucijoje turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per metus. Saugos dokumentai turi būti persvarstomi (peržiūrimi) po rizikos analizės ar informacinių technologijų saugos atitikties vertinimo atlikimo arba valstybės institucijoje įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams. Prireikus saugos dokumentai turi būti tikslinami ir derinami su Vidaus reikalų ministerija.

## V. SAUGOS INCIDENTŲ VALDYMAS

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

28. Administratorius arba informacinių technologijų pagalbos tarnyba apie šių Reikalavimų 27 punkte nurodytus pažeidimus informuoja saugos įgaliotinį. Įtaręs neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeisiančią informacinės sistemos saugą (jos konfidencialumą, vientisumą ar prieinamumą), saugos įgaliotinis apie tai turi pranešti kompetentingoms institucijoms.

29. Informacijos saugos incidentų, įvykusių informacinėje sistemoje, tyrimo tvarka nustatoma Informacinės sistemos veiklos tęstinumo valdymo plane.

*Punkto pakeitimai:*

Nr. [743](#), 2008-07-16, Žin., 2008, Nr. 85-3393 (2008-07-26), i. k. 1081100NUTA00000743

## VI. RIZIKOS ĮVERTINIMAS

30. Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą 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. [743](#), 2008-07-16, Žin., 2008, Nr. 85-3393 (2008-07-26), i. k. 1081100NUTA00000743

31. Informacinių sistemų rizikos įvertinimas išdėstomas rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausieji rizikos veiksniai yra šie:

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

31.2. subjektyvūs tyčiniai (nesankcionuotas naudojimas informacine sistema duomenims gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

31.3. nenugalima jėga (*force majeure*).

32. 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.

## VII. INFORMACINĖS SISTEMOS FUNKCIJŲ POKYČIŲ VALDYMAS

33. Informacinės sistemos valdytojas užtikrina efektyvų ir spartų informacinės sistemos funkcijų pokyčių (toliau vadinama – pokyčiai) valdymo planavimą, apimančią pokyčių identifikavimą, suskirstymą į kategorijas, įtakos vertinimą ir pokyčių prioritetų nustatymo procesus. Su tuo susijusios nuostatos numatomos informacinės sistemos valdytojo tvirtinamoje Informacinės sistemos pokyčių valdymo tvarkoje arba Saugaus elektroninės informacijos tvarkymo taisyklėse.

*Punkto pakeitimai:*

Nr. [743](#), 2008-07-16, Žin., 2008, Nr. 85-3393 (2008-07-26), i. k. 1081100NUTA00000743

34. Asmuo, inicijuojantis pokytį, be informacinės sistemos valdytojo vadovo rašytinio leidimo negali pokyčio pats įgyvendinti.

35. Funkcijos, susijusios su informacinės sistemos plėtra, turi būti aiškiai atskirtos nuo administravimo (eksplotavimo) funkcijų.

36. Informacinės sistemos sąrankos dokumentacija turi būti nuolat atnaujinama ir rodyti esamą informacinės sistemos sąrankos būklę.

37. Pokyčiai, galintys turėti neigiamą įtaką informacinės sistemos konfidencialumui, vientisumui ar prieinamumui, turi būti patikrinti bandomojoje aplinkoje, kurioje nėra konfidencialių duomenų ir kuri atskirta nuo eksploatuojamos informacinės sistemos.

## VIII. INFORMACINIŲ TECHNOLOGIJŲ SAUGOS ATITIKTIES VERTINIMAS

38. Teisės aktų nustatyta tvarka atliekant informacinių technologijų saugos atitikties vertinimą, rekomenduojama:

38.1. įvertinti saugos dokumentų ir realios informacijos saugos situacijos atitiktį;

38.2. inventorizuoti informacinės sistemos techninę ir programinę įrangą;

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

38.4. patikrinti (įvertinti) informacinės sistemos naudotojams suteiktų teisių ir vykdomų funkcijų atitiktį;

38.5. įvertinti pasirengimą užtikrinti informacinės sistemos veiklos tęstinumą įvykus saugos incidentui.

39. Atlikus šių Reikalavimų 38 punkte nurodytą vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato informacinės sistemos valdytojo vadovas.

## IX. INFORMACINĖS SISTEMOS NAUDOTOJŲ ATSAKOMYBĖ

40. Informacinės sistemos naudotojai privalo rūpintis informacinės sistemos ir joje tvarkomos informacijos saugumu.

41. Tvarkyti informacinės sistemos duomenis gali tik informacinės sistemos naudotojai, susipažinę su saugos dokumentais ir raštu sutikę laikytis jų reikalavimų.

42. Informacinės sistemos naudotojus su saugos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą pasirašytinai supažindina saugos įgaliotinis.

43. Informacinės sistemos naudotojai, pažeidę šių Reikalavimų ir kitų saugų informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako įstatymų nustatyta tvarka.

---

**Pakeitimai:**

1.

Lietuvos Respublikos Vyriausybė, Nutarimas

Nr. [2105](#), 2002-12-31, Žin., 2003, Nr. 2-45 (2003-01-08), i. k. 1021100NUTA00002105

Dėl Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimo Nr. 952 "Dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemose" pakeitimo

2.

Lietuvos Respublikos Vyriausybė, Nutarimas

Nr. [410](#), 2007-04-25, Žin., 2007, Nr. 49-1891 (2007-05-05), i. k. 1071100NUTA00000410

Dėl Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimo Nr. 952 "Dėl duomenų saugos valstybės ir savivaldybių informacinėse sistemose" pakeitimo

3.

Lietuvos Respublikos Vyriausybė, Nutarimas

Nr. [743](#), 2008-07-16, Žin., 2008, Nr. 85-3393 (2008-07-26), i. k. 1081100NUTA00000743

Dėl Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimo Nr. 952 "Dėl elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose" pakeitimo

4.

Lietuvos Respublikos Vyriausybė, Nutarimas

Nr. [519](#), 2011-05-04, Žin., 2011, Nr. 55-2642 (2011-05-10), i. k. 1111100NUTA00000519

Dėl Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimo Nr. 952 "Dėl elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose" pakeitimo