LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTRAS

Į S A K Y M A S
DĖL TIPINIŲ DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2003 m. liepos 16 d. Nr. 1V-272
Vilnius

Įgyvendindamas Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimo Nr. 952 „Dėl duomenų saugos valstybės ir savivaldybių informacinėse sistemose“ (Žin., 1997, Nr. 83-2075; 2003, Nr. 2-45) 3 punktą,

t v i r t i n u Tipinius duomenų saugos nuostatus (pridedama).

VIDAUS REIKALŲ MINISTRAS VIRGILIJUS BULOVAS

_____

PATVIRTINTA

Lietuvos Respublikos vidaus reikalų ministro
2003 m. liepos 16 d. įsakymu Nr. 1V-272

TIPINIAI DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Tipinių duomenų saugos nuostatų (toliau – nuostatai) tikslas – sudaryti sąlygas saugiai automatizuotu būdu tvarkyti duomenis valstybės registruose ar kitose informacinėse sistemose (toliau – sistema).

2. Sistemos valdytojas, vadovaujančioji valstybės registro tvarkymo įstaiga arba, jeigu jos nėra, valstybės registro tvarkymo įstaiga (toliau – sistemos tvarkytojas), pagal kompetenciją, vadovaudamasis Tipiniais duomenų saugos nuostatais, rengia ir suderinęs su Vidaus reikalų ministerija tvirtina sistemos duomenų saugos nuostatus, kurie kartu su rengtinomis detaliomis instrukcijomis, procedūrų aprašymais ir saugaus darbo su duomenimis tvarkos taisyklėmis apibrėžia sistemos saugumo politiką (toliau – saugumo politika).

II. SISTEMOS APIBŪDINIMAS

3. Nuostatai reglamentuoja sistemos automatizuotą duomenų apdorojimą ir yra privalomi visiems valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartis, sistemos tvarkytojo įstaigoje (toliau – sistemos vartotojas).

4. Sistemos apibūdinimas. Tvarkomų duomenų grupių aprašymas.

5. Sistemą sudaro šios posistemės ir paslaugos:

5.1. (pavadinimas), skirtos ar vykdančios (aprašymas).

6. Saugų sistemos duomenų tvarkymą reglamentuoja:

6.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (Žin., 1996, Nr. 63-1479; 2000, Nr. 64-1924; 2003, Nr. 15-597);

6.2. Bendrieji duomenų saugos reikalavimai, patvirtinti Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 „Dėl duomenų saugos valstybės ir savivaldybių informacinėse sistemose“ (Žin., 1997, Nr. 83-2075; 2003, Nr. 2-45) (toliau – Bendrieji duomenų saugos reikalavimai);

6.3. Lietuvos standartas LST ISO/IEC 17799:2002, Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo technika“ grupės standartai, reglamentuojantys saugų duomenų tvarkymą;

6.4. kiti teisės aktai, reglamentuojantys duomenų tvarkymo teisėtumą, sistemos tvarkytojo veiklą bei duomenų saugos valdymą.

III. DUOMENŲ SAUGOS ORGANIZAVIMAS IR NENUMATYTŲ SITUACIJŲ VALDYMAS

7. Už duomenų tvarkymo teisėtumą ir duomenų saugą atsako sistemos tvarkytojas.

8. Tvirtindamas nuostatus ir kitus saugumo politiką reglamentuojančius teisės aktus, sistemos tvarkytojas skiria saugos įgaliotinį, kuris atsako už saugumo politikos įgyvendinimą ir kontrolę. Sistemos tvarkytojo sprendimu saugumo politikai įgyvendinti ir saugumo kontrolei užtikrinti gali būti steigiamas atskiras padalinys.

9. Saugos įgaliotinis teikia siūlymus sistemos tvarkytojui dėl atskirų sistemos posistemių ar funkcijų administratorių (toliau – administratorius), kurie už paskirtų funkcijų vykdymą atsiskaito tiesiogiai saugos įgaliotiniui, paskyrimo.

10. Sistemos vartotojai turi turėti atitinkamą kvalifikaciją (kvalifikacijos kėlimo kursai, pradinis saugaus darbo su duomenimis mokymas, ECDL vartotojo sertifikatas ar pan.) ir patirties

(dirbant su tinkamomis operacinėmis sistemomis, taikomosiomis programomis ir pan.). Aukštesni nei sistemos vartotojams reikalavimai turi būti nustatyti saugos įgaliotiniui ir administratoriams.

11. Sistemos vartotojai, pastebėję saugumo politikos pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti atitinkamos funkcijos administratoriui, o jo nesant – saugos įgaliotiniui.

12. Sistemos vartotojų veiksmus esant nenumatytai situacijai reglamentuoja nenumatytų situacijų valdymo planas (toliau – planas), kurį sistemos tvarkytojo vadovui teikia tvirtinti saugos įgaliotinis. Plano nuostatos pagrįstos šiais principais:

12.1. sistemos vartotojų gyvybės ir sveikatos apsauga. Būtina užtikrinti visų sistemos vartotojų gyvybės ir sveikatos apsaugą bei saugumą, kol trunka nenumatyta situacija ir likviduojami avarijų padariniai;

12.2. sistemos veiklos atstatymas. Paskelbus apie avariją, organizuojamas sistemos veiklos atstatymas, o esant sutrikimų, atstatymas organizuojamas tik pagal planą. Visų pirma turi būti atkurtos pagrindinės sistemos funkcijos;

12.3. sistemos vartotojų mokymas. Sistemos vartojai turi būti supažindinti su planu ir su teisės aktais, nustatančiais asmeninę kiekvieno sistemos vartotojo atsakomybę. Plano arba jo dalių vykdymas turi būti išbandytas realiuose mokymuose.

IV. RIZIKOS ĮVERTINIMAS IR DETALI DARBO TVARKA

13. Pagrindinės sistemos rizikos mažinimo priemonės išdėstomos rizikos ataskaitoje, kuri rengiama įvertinus Bendrųjų duomenų saugos nuostatų 10 punkte nustatytus rizikos veiksnius (toliau – rizikos veiksniai).

14. Konkrečios sistemos duomenų tvarkymo ir saugumo procedūros išdėstomos detaliose darbo su duomenimis taisyklėse (toliau – taisyklės) (jos gali būti išdėstomos nuostatuose arba kaip atskiri teisės aktai (tai nurodoma nuostatuose), kurias sistemos tvarkytojo vadovui teikia tvirtinti saugos įgaliotinis. Taisykles sudaro:

14.1. techninės, programinės ir fizinės duomenų saugos priemonės (atsarginis elektros energijos tiekimas, antivirusinė programinė įranga, duomenų šifravimas, kompiuterinių tinklų apsaugos sistema, darbo apskaita, patalpų fizinė sauga ir kita);

14.2. prieinamumo prie duomenų principai ir kontrolė (sistemos vartotojų registravimas, teisės dirbti su sistemos duomenimis suteikimas, sistemos vartotojų išregistravimas, sistemos vartotojų tapatybės nustatymas, specialios sistemos vartotojų tapatybės nustatymo priemonės, elektroninis parašas ir kita);

14.3. sistemos ir duomenų vientisumo pažeidimų fiksavimo ir pažeistų duomenų atkūrimo tvarka (sistemos vartotojų veiksmų registravimas, atsarginės duomenų kopijos ir jų saugojimas bei saugojimo kontrolė, duomenų atkūrimo tvarka ir kita);

14.4. saugaus duomenų teikimo duomenų vartotojams tvarka ir kontrolė;

14.5. saugaus duomenų perkėlimo ar perdavimo tvarka ir jos laikymosi kontrolė;

14.6. įgaliojimai sistemos tvarkytojui ir jo teisės.

V. SISTEMOS VARTOTOJŲ ATSAKOMYBĖ

15. Sistemos vartotojai privalo rūpintis sistemos bei joje tvarkomų duomenų saugumu.

16. Tvarkyti sistemos duomenis gali tik sistemos vartotojai, susipažinę su šiais nuostatais ir kitais saugumo politiką reglamentuojančiais teisės aktais bei raštiškai sutikę laikytis šių teisės aktų reikalavimų.

17. Sistemos vartotojų supažindinimą su nuostatais ir kitais saugumo politiką reglamentuojančiais teisės aktais bei atsakomybę už šių reikalavimų nesilaikymą pasirašytinai organizuoja saugos įgaliotinis.

18. Sistemos vartotojams turi būti nuolat rengiami duomenų saugos mokymai, įvairiais būdais primenama apie saugumo problematiką (pvz., priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės naujai priimtiems darbuotojams ir pan.).

19. Sistemos vartotojai, pažeidę šių nuostatų ar kitų saugumo politiką reglamentuojančių teisės aktų reikalavimus, atsako įstatymų nustatyta tvarka.

VI. NUOSTATŲ ATNAUJINIMO TVARKA

20. Saugos įgaliotinis, siekdamas užtikrinti sistemos ir joje tvarkomų duomenų saugumą, teikia siūlymus sistemos tvarkytojo vadovui dėl nuostatų keitimo ar kitų saugumo politiką reglamentuojančių teisės aktų priėmimo, keitimo ar panaikinimo.

21. Nuostatai ir kiti saugumo politiką reglamentuojantys teisės aktai iš esmės peržiūrimi ir prireikus keičiami ne rečiau kaip kartą per metus atliekant šių nuostatų VII skirsnyje nurodytą auditą.

VII. BAIGIAMOSIOS NUOSTATOS

22. Siekiant užtikrinti nuostatuose ir kituose saugumo politiką reglamentuojančiuose teisės aktuose išdėstytų nuostatų įgyvendinimo kontrolę, saugos įgaliotinis kasmet organizuoja auditą, kurio metu:

22.1. įvertinama nuostatų ir kitų saugumo politiką reglamentuojančių teisės aktų atitiktis realiai duomenų saugos situacijai;

22.2. inventorizuojama sistemos tvarkytojo techninė ir programinė įranga;

22.3. tikrinamos ne mažiau kaip 10-yje procentų sistemos vartotojų kompiuterinių darbo vietų ir visuose paslaugų kompiuteriuose įdiegtos programos ir jų konfigūracija;

22.4. peržiūrima sistemos vartotojams suteiktų teisių atitiktis vykdomoms funkcijoms;

22.5. įvertinamas pasiruošimas sistemos veiklos atstatymui nenumatytose situacijose.

23. Atlikus auditą rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato sistemos tvarkytojo vadovas.

_____