LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTRAS

Į S A K Y M A S
DĖL LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTRAS 2007 M. SAUSIO 2 D. ĮSAKYMO NR. 1V-1 „DĖL VIDAUS REIKALŲ INFORMACINĖS SISTEMOS NUOSTATŲ IR VIDAUS REIKALŲ INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO

2007 m. spalio 23 d. Nr. 1V-367
Vilnius

Vadovaudamasis Lietuvos Respublikos Vyriausybės 2007 m. balandžio 25 d. nutarimo Nr. 410 „Dėl Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimo Nr. 952 „Dėl duomenų saugos valstybės ir savivaldybių informacinėse sistemose“ pakeitimo“ (Žin., 2007, Nr. 49-1891) 2 punktu, Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų, patvirtintų Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891), 6.1, 8 ir 15 punktais:

1. P a k e i č i u Lietuvos Respublikos vidaus reikalų ministro 2007 m. sausio 2 d. įsakymą Nr. 1V-1 „Dėl Vidaus reikalų informacinės sistemos nuostatų ir Vidaus reikalų informacinės sistemos duomenų saugos nuostatų patvirtinimo“ (Žin., 2007, Nr. 3-141):

1.1. Išdėstau preambulę taip:

„Vadovaudamasis Valstybės informacinių sistemų steigimo ir įteisinimo taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 2004 m. balandžio 19 d. nutarimu Nr. 451 (Žin., 2004, Nr. 58-2061), 8 punktu, Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų, patvirtintų Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891), 6.1 punktu bei atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministro 2005 m. gruodžio 20 d. įsakymą Nr. 1V-425 „Dėl Vidaus reikalų informacinės sistemos“:“;

1.2. išdėstau nurodytuoju įsakymu patvirtintus Vidaus reikalų informacinės sistemos duomenų saugos nuostatus nauja redakcija (pridedama).

2. S k i r i u Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktorių Vygantą Ivanauską Vidaus reikalų informacinės sistemos saugos įgaliotiniu.

3. P a v e d u Informatikos ir ryšių departamentui prie Lietuvos Respublikos vidaus reikalų ministerijos iki š. m. gruodžio 30 d. teisės aktų nustatyta tvarka parengti ir pateikti tvirtinti vidaus reikalų ministrui teisės aktų projektus dėl:

3.1. Vidaus reikalų informacinės sistemos duomenų saugaus tvarkymo;

3.2. Vidaus reikalų informacinės sistemos veiklos tęstinumo valdymo;

3.3. Vidaus reikalų informacinės sistemos centrinio duomenų banko vartotojų administravimo;

3.4. Vidaus reikalų informacinės sistemos duomenų saugos incidentų tyrimo;

3.5. Vidaus reikalų informacinės sistemos pokyčių valdymo.

VIDAUS REIKALŲ MINISTRAS RAIMONDAS ŠUKYS

PATVIRTINTA
Lietuvos Respublikos vidaus reikalų ministro
2007 m. sausio 2 d. įsakymu Nr. 1V-1
(Lietuvos Respublikos vidaus reikalų ministro
2007 m. spalio 23 d. įsakymo Nr. 1V-367
redakcija)

VIDAUS REIKALŲ INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Vidaus reikalų informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Vidaus reikalų informacinės sistemos (toliau – VRIS) saugos politiką.

2. Šiuose Saugos nuostatuose vartojamos sąvokos atitinka Bendruosiuose elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuose, patvirtintuose Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891) (toliau – Saugos reikalavimai), Vidaus reikalų informacinės sistemos nuostatuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2007 m. sausio 2 d. įsakymu Nr. 1V-1 (Žin., 2007, Nr. 3-141) (toliau – VRIS nuostatai), Saugos dokumentų turinio gairėse, patvirtintose Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070), ir kituose teisės aktuose vartojamas sąvokas.

3. VRIS saugos tikslas – užtikrinti VRIS centrinio duomenų banko (toliau – VRIS CDB) duomenų konfidencialumą, prieinamumą ir vientisumą.

4. VRIS CDB duomenų saugos užtikrinimo prioritetinės kryptys:

4.1. VRIS CDB duomenų tvarkymui naudojamos techninės ir programinės įrangos kontrolė;

4.2. VRIS CDB duomenų tvarkymo kontrolė;

4.3. Naudojimosi VRIS CDB duomenimis kontrolė.

5. VRIS CDB duomenų saugumui užtikrinti kompleksiškai naudojamos administracinės, techninės ir programinės priemonės.

6. Saugos nuostatai taikomi:

6.1. VRIS valdytojai – Lietuvos Respublikos vidaus reikalų ministerijai (toliau – VRM), kuri:

6.1.1. priima sprendimą dėl VRIS informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

6.1.2. atlieka kitas Saugos nuostatų, Saugos reikalavimų, VRIS nuostatų ir kitų teisės aktų nustatytas funkcijas.

6.2. VRIS tvarkytojui – Informatikos ir ryšių departamentui prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – IRD), kuris:

6.2.1. atsako už VRIS CDB duomenų tvarkymo teisėtumą ir duomenų saugą;

6.2.2. atlieka kitas Saugos nuostatų, Saugos reikalavimų, VRIS nuostatų ir kitų teisės aktų nustatytas funkcijas, susijusias su VRIS CDB duomenų sauga.

6.3. kitiems VRIS tvarkytojams – VRIS registrų ir informacinių sistemų tvarkymo įstaigoms ir VRM reguliavimo srities įstaigoms, kurių informacija talpinama į VRM tinklalapį.

7. Saugos įgaliotinis atlieka Saugos nuostatų, Saugos reikalavimų ir kitų teisės aktų nustatytas funkcijas.

8. Įstaigų prie VRM valdomų valstybės ir žinybinių registrų ir informacinių sistemų, sudarančių VRIS informacinę infrastruktūrą, duomenų saugą užtikrina šių registrų ir informacinių sistemų saugos įgaliotiniai ir administratoriai šių registrų ir informacinių sistemų duomenų saugos nuostatų nustatyta tvarka.

9. VRIS posistemių ir funkcijų administratoriai atlieka VRIS priežiūrą, teikia siūlymus VRIS saugos įgaliotiniui dėl VRIS saugos priemonių, atlieka kitas Saugos reikalavimų, kitų teisės aktų nustatytas funkcijas.

10. Teisės aktai, kuriais vadovaujantis tvarkomi VRIS CDB duomenys ir užtikrinama jų sauga:

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

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

10.3. Saugos reikalavimai;

10.4. VRIS nuostatai;

10.5. VRM ir įstaigų prie VRM valdomų valstybės ir žinybinių registrų bei informacinių sistemų nuostatai bei duomenų saugos nuostatai, VRIS posistemių duomenų tvarkymą reglamentuojantys teisės aktai;

10.6. Lietuvos standartai LST ISO/IEC 17799: 2005 ir LST ISO/IEC 27001: 2006 bei Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, reglamentuojantys saugų duomenų tvarkymą;

10.7. kiti teisės aktai, reglamentuojantys VRIS CDB duomenų tvarkymo teisėtumą, VRIS tvarkytojų veiklą ir VRIS CDB duomenų saugos valdymą.

II. VRIS CDB DUOMENŲ SAUGOS VALDYMAS

11. Atsižvelgiant į VRIS CDB duomenų savybių (vientisumo, konfidencialumo ir prieinamumo) įtaką VRIS darbui, VRIS priskiriama antrajai informacinių sistemų kategorijai pagal Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairių, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymu Nr. 1V-247 (Žin., 2007, Nr. 78-3160), 3.1.1 punktą.

12. VRIS saugos priemonės parenkamos įvertinus galimus rizikos veiksnius VRIS CDB duomenų vientisumui, konfidencialumui ir prieinamumui.

13. Pagrindinės VRIS rizikos mažinimo priemonės išdėstomos rizikos įvertinimo ataskaitoje, kurią kasmet iki liepos 1 dienos, o prireikus ir neeilinio rizikos įvertinimo ataskaitą iki VRIS valdytojo nurodytos datos rengia saugos įgaliotinis, įvertinęs galinčius turėti įtakos VRIS CDB duomenų saugai rizikos veiksnius, iš kurių svarbiausieji išvardyti Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų 31 punkte.

14. VRIS valdytojas, atsižvelgdamas į VRIS rizikos įvertinimo ataskaitą, prireikus tvirtina IRD parengtą rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

15. VRIS rizikos veiksnių vertinimui taikoma kokybinė rizikos vertinimo metodika.

16. Pagrindiniai rizikos kriterijai pasirenkami atliekant VRIS rizikos įvertinimą priklausomai nuo VRIS rizikos vertinimo strategijos.

17. Siekiant užtikrinti Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose išdėstytų nuostatų įgyvendinimo kontrolę, vidaus reikalų ministro patvirtintos informacinių technologijų saugos atitikties vertinimo metodikos nustatyta tvarka kasmet organizuojamas VRIS informacinių technologijų saugos reikalavimų atitikties vertinimas, kurio metu:

17.1. įvertinama Saugos nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų atitiktis realiai VRIS CDB duomenų saugos situacijai;

17.2. inventorizuojama VRIS techninė ir programinė įranga;

17.3. tikrinama ne mažiau kaip 10 procentų VRIS CDB vartotojų kompiuterizuotų darbo vietų ir VRIS CDB tarnybinėse stotyse įdiegtos programos bei jų sąranka (konfigūracija);

17.4. patikrinama VRIS CDB vartotojams suteiktų teisių tvarkyti VRIS CDB atitiktis atliekamoms funkcijoms, prireikus VRIS CDB vartotojų teisės praplečiamos ar apribojamos;

17.5. įvertinamas pasiruošimas atkurti VRIS veiklą VRIS CDB duomenų saugos incidento atveju.

18. Atlikus VRIS informacinių technologijų saugos reikalavimų atitikties vertinimą,

rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato VRIS valdytojas.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

19. VRIS CDB darbui turi būti naudojama tik legali programinė įranga.

20. VRIS CDB tarnybinėse stotyse neturi veikti programinė įranga, nesusijusi su VRIS CDB duomenų tvarkymu, VRIS CDB vartotojų ir pačios įrangos administravimu.

21. VRIS CDB tarnybinėse stotyse privalo būti naudojama programinė įranga, skirta kovai su kenksminga programine įranga, atnaujinama automatiniu būdu ne rečiau kaip kas trys dienos.

22. VRIS CDB programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims.

23. VRIS naudojamas Vidaus reikalų telekomunikacinis tinklas, už kurio administravimą ir priežiūrą atsako šio tinklo pagrindinis tvarkytojas, turi būti atskirtas nuo kitų tinklų tinklo užkarda.

24. VRIS CDB vartotojų, jų vykdytų užklausų ir peržiūrėtų užklausų rezultatų duomenys tvarkomi VRIS CDB vartotojų administravimo posistemėje vidaus reikalų ministro nustatyta tvarka.

25. Tiesioginė prieiga prie VRIS CDB duomenų suteikiama įgyvendinus VRIS CDB vartotojų autentifikavimo priemones. Tiesioginė prieiga prie VRIS CDB duomenų užtikrinama automatiniu būdu ištisą parą darbo ir poilsio dienomis.

26. VRIS CDB duomenys perduodami automatiniu būdu naudojant TCP/IP protokolą realiame laike („On-line“ režimu) arba asinchroniniu režimu pagal VRIS CDB duomenų teikimo sutartis, kuriose nustatytos perduodamų duomenų specifikacijos, kopijų skaičius, kitos duomenų perdavimo sąlygos ir tvarka.

27. VRIS CDB duomenys, perduodami ne per VRM priklausančias duomenų perdavimo linijas, turi būti šifruojami; duomenų šifravimą privalo užtikrinti VRIS valdytojas ir VRIS tvarkytojai, atsakingi už VRIS CDB duomenų saugą; VRIS CDB duomenų gavėjų prieigą prie VRIS CDB duomenų turi kontroliuoti tinklo užkarda.

28. VRIS CDB vartotojams, savo tarnybinėms funkcijoms vykdyti naudojantiems nešiojamus kompiuterius VRIS CDB duomenų perdavimui kompiuterių tinklais ne savo darbo vietoje, šiuose kompiuteriuose turi būti naudojamas kompiuterio įjungimo slaptažodis, papildomas VRIS CDB vartotojo tapatybės patvirtinimas ir VRIS CDB duomenų šifravimas.

29. VRIS CDB duomenų kopijos turi būti daromos automatiškai kiekvieną dieną. Prireikus jas atkurti turi teisę atitinkamos funkcijos administratorius.

IV. REIKALAVIMAI PERSONALUI IR SUPAŽINDINIMO SU SAUGOS REIKALAVIMAIS TVARKA

30. Saugos įgaliotinis privalo turėti dokumentais patvirtintą informacinių technologijų specialisto kvalifikaciją, išmanyti informacinių sistemų administravimą, gerai žinoti elektroninės informacijos saugos principus bei saugos užtikrinimo metodus.

31. VRIS posistemių ir funkcijų administratoriai privalo išmanyti pagrindinius saugos politikos principus, darbą su duomenų perdavimo tinklais, užtikrinti jų saugumą, turėti sisteminių programinių priemonių (*Windows, Unix, Oracle*) administravimo bei priežiūros patirties.

32. VRIS CDB vartotojai turi turėti atitinkamą kvalifikaciją (informacinių technologijų vartotojų kvalifikacijos kursai, pradinis saugaus darbo su duomenimis mokymas, ECDL (Europos kompiuterio vartotojo pažymėjimas) vartotojo sertifikatas ar pan.) ir patirties (dirbant su atitinkamomis operacinėmis sistemomis, taikomosiomis programomis ir pan.).

33. Tvarkyti VRIS CDB duomenis gali tik VRIS CDB vartotojai, pasirašytinai susipažinę su Saugos nuostatais ir kitais saugos politiką įgyvendinančiais teisės aktais.

34. VRIS CDB vartotojų supažindinimą su Saugos nuostatais ir kitais saugos politiką įgyvendinančiais teisės aktais ir atsakomybe už šių reikalavimų nesilaikymą organizuoja saugos įgaliotinis. Saugos įgaliotinis raštu informuoja VRIS CDB vartotojus apie Saugos nuostatų

pakeitimus ar kitų saugos politiką įgyvendinančių teisės aktų pripažinimą netekusiais galios, keitimą ar priėmimą.

35. VRIS CDB vartotojams turi būti nuolat rengiami duomenų saugos mokymai, įvairiais būdais primenama apie saugos problematiką (pvz., priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės ir pan.).

V. BAIGIAMOSIOS NUOSTATOS

36. VRIS saugos įgaliotinis, VRIS funkcijų ir posistemių administratoriai, VRIS CDB vartotojai, pažeidę Saugos nuostatų ar kitų saugos politiką įgyvendinančių teisės aktų reikalavimus, atsako įstatymų nustatyta tvarka.

_____