VYRIAUSYBINIŲ RYŠIŲ CENTRO
PRIE LIETUVOS RESPUBLIKOS VALSTYBĖS SAUGUMO DEPARTAMENTO
DIREKTORIUS

ĮSAKYMAS
DĖL VALSTYBĖS INSTITUCIJŲ RYŠIO TINKLO SAUGOS NUOSTATŲ PATVIRTINIMO

2011 m. birželio 3 d. Nr. 1-18
Vilnius

Vadovaudamasis Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 8 d. nutarimu Nr. 972 „Dėl valstybinių institucijų ryšių tobulinimo“ (Žin., 1997, Nr. 84-2109):

1. T v i r t i n u Valstybės institucijų ryšio tinklo saugos nuostatus (pridedama).

2. N u r o d a u paskelbti šį įsakymą Vyriausybinių ryšių centrui prie Lietuvos Respublikos valstybės saugumo departamento interneto tinklapyje.

3. P a v e d u įsakymo vykdymo kontrolę Komutacinių įrenginių skyriaus viršininkui Almantui Burauskui.

L. e. direktoriaus pareigas Vytautas Janušis

Parengė
Almantas Burauskas
2011-06- 03

PATVIRTINTA
Vyriausybinių ryšių centro prie Lietuvos Respublikos valstybės saugumo departamento direktoriaus 2011 m. birželio 3 d. įsakymu Nr. 1-18

VALSTYBĖS INSTITUCIJŲ RYŠIO TINKLO SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Valstybės institucijų ryšio tinklo saugos nuostatų (toliau – Saugos nuostatai) tikslas – nustatyti ir įgyvendinti organizacines, technines ir kitas priemones, sudarančias sąlygas nepertraukiamai tiekti elektroninių ryšių paslaugas Valstybės institucijų ryšio tinklo (toliau – VIRT) naudotojams, saugiai tvarkyti (rinkti, apdoroti, kaupti, saugoti) VIRT srauto duomenis bei teikti juos suinteresuotiems asmenims.

2. Saugos nuostatai parengti vadovaujantis 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), Saugos dokumentų turinio gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070), Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniais saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2008 m. spalio 27 d. įsakymu Nr. 1V-384, 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).

3. Saugos nuostatai privalomi visiems VIRT valdytojo atsakingiems asmenims, VIRT saugos įgaliotiniui, VIRT administratoriams, VIRT duomenų srauto tvarkytojams.

II. VIRT SAUGOS POLITIKOS TIKSLAI IR PRIORITETINĖS KRYPTYS

4. VIRT saugos politikos tikslai:

4.1. užtikrinti nepertraukiamą VIRT funkcionavimą;

4.2. užtikrinti VIRT srauto duomenų konfidencialumą, patikimumą, pasiekiamumą.

5. VIRT saugos užtikrinimo prioritetinės kryptys:

5.1. VIRT komutavimo įrenginių, jungiamųjų ryšio linijų, VIRT srauto duomenų tvarkymo techninių priemonių ir duomenų bazių fizinės saugos užtikrinimas;

5.2. VIRT srauto duomenų tvarkymo techninių priemonių bei programinės įrangos naudojimo kontrolė;

5.3. organizacinių VIRT srauto duomenų tvarkymo priemonių parengimas, įgyvendinimas, kontrolė.

6. VIRT srauto duomenys tvarkomi ketvirtos kategorijos pagal „Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gaires“, patvirtintas Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymu Nr. 1V-247 (Žin., 2007, Nr. 78-3160; 2008, 127-4866), informacinėje sistemoje.

7. VIRT srauto duomenų sauga užtikrinama vadovaujantis Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, Saugos dokumentų turinio gairėmis, Lietuvos Respublikos standartu LST ISO/IEC 17799:2006, „Informacijos technologija. Praktiniai informacijos saugumo valdymo aspektai“, Lietuvos Respublikos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais, šiais Saugos nuostatais, VIRT nuostatais, VIRT Administravimo taisyklėmis, kitais teisės aktais.

III. VIRT VALDYTOJAS IR VIRT SRAUTO DUOMENŲ TVARKYTOJAI

8. VIRT valdytojas – Vyriausybinių ryšių centras prie Lietuvos Respublikos valstybės saugumo departamento (toliau – VRC). Buveinės adresas – Gedimino pr. 40/1, LT-01110 Vilnius.

9. VIRT srauto duomenų tvarkytojai:

9.1. pagrindinis tvarkytojas – VRC Komutacinių įrenginių skyrius (toliau – KĮS). Buveinės adresas – Gedimino pr. 40/1 LT-01110 Vilnius;

9.2. Kitas VIRT srauto duomenų tvarkytojas – VRC Linijinis abonentinis skyrius (toliau – LAS). Buveinės adresas – Gedimino pr. 40/1, LT-01110 Vilnius.

10. VIRT valdytojo ir VIRT srauto duomenų tvarkytojų uždaviniai, funkcijos, pareigos ir teisės nurodytos VIRT nuostatuose ir VIRT administravimo taisyklėse.

IV. VIRT SAUGOS ĮGALIOTINIS IR VIRT SRAUTO DUOMENŲ ADMINISTRATORIUS

11. VIRT saugos įgaliotinį ir VIRT srauto duomenų administratorių įsakymu skiria VRC direktorius.

12. VIRT saugos įgaliotinis (toliau – Saugos įgaliotinis):

12.1. pagal kompetenciją organizuoja ir kontroliuoja VIRT saugos politiką reglamentuojančių teisės aktų įgyvendinimą ir už tai atsako;

12.2. pagal kompetenciją instruktuoja VIRT srauto duomenų tvarkytojus ir VIRT srauto duomenų administratorius (toliau – Administratorius);

12.3. pagal kompetenciją teikia VIRT srauto duomenų tvarkytojams ir Administratoriui privalomus vykdyti nurodymus;

12.4. informuoja VRC direktorių arba jo įgaliotą asmenį apie VIRT saugos politikos pažeidimus ir koordinuoja įvykusių VIRT saugos incidentų tyrimą;

12.5. pagal kompetenciją teikia VRC direktoriui arba jo įgaliotam asmeniui pasiūlymus dėl:

12.5.1. VIRT srauto duomenų tvarkytojų ir Administratoriaus skyrimo;

12.5.2. VIRT saugos politiką reglamentuojančių aktų priėmimo, keitimo ar panaikinimo;

12.5.3. VIRT atitikimo nustatytiems saugos reikalavimams atitikties vertinimo atlikimo;

12.6. pagal kompetenciją atlieka kitas VIRT saugos politiką įgyvendinančiuose teisės aktuose nustatytas funkcijas;

12.7. vykdo kitus VRC direktoriaus arba jo įgalioto asmens nurodymus, susijusius su VIRT saugos politikos įgyvendinimu.

13. Administratorius:

13.1. pagal kompetenciją suteikia paskirtiesiems VIRT srauto duomenų tvarkytojams prieigą prie VIRT srauto duomenų;

13.2. pagal kompetenciją administruoja VIRT srauto duomenų tvarkymo informacinės sistemos elementus (kompiuterius, operacines sistemas, duomenų bazių valdymo sistemas, taikomųjų programų sistemas, ugniasienes, duomenų perdavimo tinklus);

13.3. registruoja įvykusius VIRT saugos incidentus ir informuoja apie juos Saugos įgaliotinį, pagal kompetenciją dalyvauja jų tyrime ir teikia pasiūlymus dėl saugos incidentų šalinimo bei prevencijos priemonių;

13.4. pagal kompetenciją užtikrina VIRT srauto duomenų saugumą, patikimumą, pasiekiamumą, konfidencialumą.

14. Saugos įgaliotinio ir Administratoriaus uždaviniai, funkcijos, pareigos ir teisės nurodytos VIRT nuostatuose, VIRT administravimo taisyklėse ir šiuose Saugos nuostatuose.

V. VIRT SRAUTO DUOMENŲ INFORMACINĖS SISTEMOS RIZIKOS IR SAUGOS ATITIKTIES ĮVERTINIMAS

15. Saugos įgaliotinis, vadovaudamasis informacinių sistemų saugos politiką nustatančiais teisės aktais, Lietuvos Respublikos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais, kasmet atlieka VIRT srauto duomenų informacinės sistemos rizikos (toliau – rizikos įvertinimas) ir VIRT srauto duomenų informacinių sistemų saugos atitikties (toliau – VIRT IS įvertinimas) įvertinimus ir pateikia VRC direktoriui arba jo įgaliotam asmeniui atitinkamas įvertinimo ataskaitas.

16. Rizikos įvertinimo ataskaitoje nurodoma:

16.1. subjektyvių netyčinių veiksmų (VIRT srauto duomenų tvarkymo klaidos ir apsirikimai, neteisėtas duomenų ištrynimas, klaidingų duomenų pateikimas, techniniai sutrikimai dėl paskirtųjų asmenų netyčinių veikų ir kita) poveikio VIRT srauto duomenų saugumui, patikimumui, pasiekiamumui, konfidencialumui ir su tuo susijusios galimos žalos įvertinimas;

16.2. subjektyvių tyčinių veiksmų (neteisėtas VIRT srauto duomenų tvarkymas ir/arba atskleidimas, tyčinis pakeitimas ar sunaikinimas, techninių gedimų sukėlimas, saugos politikos nuostatų pažeidimai, vagystės ir kita) poveikio VIRT srauto duomenų saugumui, patikimumui, pasiekiamumui, konfidencialumui ir su tuo susijusios galimos žalos įvertinimas;

16.3. nenugalimos jėgos poveikio VIRT srauto duomenų saugumui, patikimumui, pasiekiamumui, konfidencialumui ir su tuo susijusios galimos žalos įvertinimas.

16.4. priemonių plano, kuriuo siekiama sumažinti galimą 16.1, 16.2, 16 punktuose nurodytų veiksnių žalą, projektą, kuriame nurodomos techninės, administracinės ir kitos rizikos valdymo priemonės.

17. VIRT IS įvertinimo ataskaitoje nurodoma:

17.1. VIRT srauto duomenų tvarkymo atitiktis (ir/arba neatitikimai) saugos politiką nustatančių teisės aktų reikalavimams;

17.2. techninės ir programinės įrangos, naudojamos VIRT srauto duomenų tvarkymui, atitiktis (ir/arba neatitikimai) saugos politiką nustatančių teisės aktų reikalavimams;

17.3. VIRT srauto duomenų tvarkyme dalyvaujantiems asmenims suteiktų įgaliojimų atitiktis (ir/arba neatitikimai) saugos politiką nustatančių teisės aktų reikalavimams;

17.4. pasirengimo vykdyti VIRT veiklos tęstinumo plane numatytas priemones būklė;

17.5. priemonių plano, kuriuo siekiama pašalinti neatitikimus, nustatytus vykdant įvertinimą pagal 17.1, 17.2, 17.3, 17.4 punktuose nurodytas sritis, projektas, kuriame nurodomos techninės, administracinės ir kitos neatitikimų pašalinimo priemonės.

18. Rizikos įvertinimo ataskaitą ir VIRT IS įvertinimo ataskaitą (toliau bendrai – ataskaitos) tvirtina VRC direktorius arba jo įgaliotas asmuo. Vadovaudamiesi patvirtintomis ataskaitomis, VIRT duomenų tvarkytojai pagal kompetenciją rengia rizikos valdymo ir neatitikčių šalinimo priemonių įgyvendinimo veiklos planus, ir, esant reikalui, atitinkamai koreguoja strateginius bei metinius pirkimų planus.

VI. VIRT SRAUTO DUOMENŲ SAUGOS UŽTIKRINIMO TECHNINĖS PROGRAMINĖS, ORGANIZACINĖS PRIEMONĖS

19. VIRT srauto duomenų saugos užtikrinimo priemonės:

19.1. patekimas į VRC ir VIRT srauto duomenų tvarkytojų patalpas kontroliuojamas ir fizinė patalpų sauga užtikrinama elektroninės durų kontrolės, vaizdo stebėjimo sistemos, elektroninės įsilaužimo ir priešgaisrinės signalizacijos priemonėmis;

19.2. prieiga prie VIRT srauto duomenų tvarkymo informacinės sistemos elementų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, duomenų perdavimo tinklų) (toliau – ISE) valdymo ir konfigūravimo suteikta tik Administratoriui;

19.3. teisė diegti programinę įrangą į ISE suteikta tik Administratoriui;

19.4. ISE naudoja iš pagrindinės VRC tarnybinės stoties valdomą antivirusinę programą, kurios duomenų bazė yra atnaujinama ne rečiau kaip kas 4 (keturias) valandas;

19.5. neteisėtų programų diegimo paiešką ISE Administratorius atlieka ne rečiau kaip vieną kartą per 6 (šešis) mėnesius;

19.6. ISE prijungti prie rezervinių maitinimo šaltinių;

19.7. ISE yra sujungti į atskirą duomenų perdavimo tinklą (potinklį) (toliau – ISE tinklas). ISE tinkle yra įdiegti metodai, suteikiantys galimybę vienareikšmiškai atpažinti ISE tinklui priklausančius kompiuterius. ISE tinkle yra nustatyti draudimai neatpažintiems naudotojams ir/arba naudotojams, dirbantiems ISE tinklui nepriklausančiais kompiuteriais prisijungti prie VIRT srauto duomenų;

19.8. atsarginės VIRT srauto duomenų kopijos:

19.8.1. daromos kiekvieną darbo dieną;

19.8.2. saugomos ne mažiau kaip 10 (dešimt) darbo dienų;

19.8.3. saugomos kitoje patalpoje nei yra įrenginys, kuriame saugomi duomenys buvo nukopijuoti;

19.8.4. atkurti duomenis iš atsarginių duomenų kopijų turi būti įmanoma per vieną darbo dieną.

19.9. prisijungimo prie VIRT srauto duomenų laikas ir trukmė VIRT srauto duomenų tvarkytojams neribojami, tačiau Administratorius gali nustatyti trukmę, po kurios VIRT srauto duomenų tvarkytojas automatiškai atjungiamas nuo VIRT srauto duomenų bazių, jei neatlieka jokių duomenų tvarkymo veiksmų;

19.10. Administratorius nustato ir valdo automatinį VIRT srauto duomenų tvarkytojų įgaliojimų patikrinimą (vartotojo vardas ir slaptažodis) prisijungimo prie VIRT srauto duomenų metu, atliekamą ISE programinėmis priemonėmis:

19.10.1. kiekvienam VIRT srauto duomenų tvarkymą atliekančiam asmeniui sukuria unikalų vartotojo vardą ir prisijungimo prie VIRT srauto duomenų slaptažodį (toliau – slaptažodis);

19.10.2. slaptažodį keičia ne rečiau kaip vieną kartą per 6 (šešis) mėnesius;

19.10.3. slaptažodį sukuria iš ne mažiau kaip 8 (aštuonių) simbolių, tarp kurių turi būti raidės (didžiosios ir/arba mažosios), skaičiai ir specialieji simboliai;

19.10.4. nustato, kad, keičiant slaptažodį, informacinė sistema neleidžia atkartoti 4 (keturių) paskutinių naudotų slaptažodžių.

20. apie ISE gedimus VIRT srauto duomenis tvarkantys asmenys nedelsdami informuoja Administratorių. Administratorius, gavęs tokį pranešimą, jį registruoja specialiame žurnale ir imasi neatidėliotinų veiksmų gedimui pašalinti.

VII. ASMENYS, DALYVAUJANTYS TVARKANT VIRT SRAUTO DUOMENIS

21. Dalyvauti tvarkant VIRT srauto duomenis gali tik VRC direktoriaus įsakymu paskirti asmenys, susipažinę su VIRT nuostatais, VIRT saugos nuostatais, VIRT administravimo taisyklėmis, informacinių sistemų saugos politiką reglamentuojančiais teisės aktais.

22. Saugos įgaliotinis privalo:

22.1. išmanyti Lietuvos Respublikos teisės aktus, nustatančiais duomenų tvarkymo saugos užtikrinimo reikalavimus ir pagal kompetenciją jais vadovautis;

22.2. išmanyti Bendruosius elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimus, patvirtintus Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891), Lietuvos Respublikos standartą LST ISO/IEC 17799:2006 „Informacijos technologija. Praktiniai informacijos saugumo valdymo aspektai“ ir pagal kompetenciją jais vadovautis;

22.3. turėti darbo su duomenų bazėmis, operacinėmis sistemomis ir taikomosiomis programomis patirties.

23. Administratorius privalo:

23.1. išmanyti Lietuvos Respublikos teisės aktus, nustatančiais duomenų tvarkymo saugos užtikrinimo principus, Bendruosius elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimus, patvirtintus Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891), būti susipažinęs su Lietuvos Respublikos standartu LST ISO/IEC 17799:2006 „Informacijos technologija. Praktiniai informacijos saugumo valdymo aspektai“ ir pagal kompetenciją jais vadovautis;

23.2. turėti duomenų perdavimo tinklų, operacinių sistemų ir programinių priemonių administravimo patirties.

24. VIRT srauto duomenis tvarkantis asmuo privalo:

24.1. turėti darbo su informacinėmis sistemomis ir jų elementais įgūdžių;

24.2. mokėti tvarkyti VIRT srauto duomenis ISE naudojamomis techninėmis ir programinėmis priemonėmis;

24.3. būti susipažinęs su elektroninių duomenų saugos politiką reglamentuojančiais teisės aktais ir pagal kompetenciją jais vadovautis.

VIII. BAIGIAMOSIOS NUOSTATOS

25. Naudotojus su šiais Saugos nuostatais pasirašytinai supažindina Saugos įgaliotinis.

26. Saugos įgaliotinis ne rečiau kaip vieną kartą per metus teikia VRC direktoriui pasiūlymus dėl šių Saugos nuostatų atnaujinimo.

27. Saugos įgaliotinis, Administratorius, VIRT srauto duomenis tvarkantys asmenys, kiti asmenys, organizuojantys, atliekantys ir/arba kontroliuojantys VIRT srauto duomenų tvarkymą, pažeidę šių Saugos nuostatų, VIRT nuostatų, VIRT administravimo taisyklių ir/arba kitų teisės aktų, reglamentuojančių VIRT valdymo ir/arba administravimo ir/arba VIRT srauto duomenų tvarkymo reikalavimus, atsako nustatyta tvarka.

28. Šiuos nuostatus įsakymu gali keisti VRC direktorius.
