PATVIRTINTA
Vyriausybinių ryšių centro prie Lietuvos Respublikos valstybės saugumo departamento direktoriaus
2010 m. spalio 15 d. įsakymu Nr.2-11RN

VYRIAUSYBINIO ŠIFRUOTO RYŠIO TINKLO DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Vyriausybinio šifruoto ryšio tinklo duomenų saugos nuostatai (toliau vadinama – Nuostatai) nustato principus ir taisykles, užtikrinančias saugų informacijos tvarkymą Vyriausybinio šifruoto ryšio tinkle (toliau vadinama – VŠR tinklas).

2. VŠR tinklo paskirtis – sudaryti sąlygas Lietuvos Respublikos paslapčių subjektams saugiai ir nenutrūkstamai tarpusavyje keistis įslaptinta arba neįslaptina tarnybine informacija. Aukščiausia leistina VŠR tinkle perduodamos ar saugomos įslaptintos informacijos slaptumo žyma – „Riboto naudojimo“.

3. Nuostatuose vartojamos sąvokos:

Informacijos tvarkymas – informacijos kūrimas, perdavimas, saugojimas; perdavimas suprantamas kaip minėtos informacijos perdavimas telekomunikacijų tinklais arba panaudojant elektronines laikmenas.

Įslaptintos informacijos saugos incidentas – įvykis ar veiksmas, kuris gali sudaryti neteisėto prisijungimo prie VŠR tinklo galimybę, sutrikdyti ar pakeisti VŠR tinklo veiklą, sunaikinti, sugadinti ar pakeisti įslaptintą informaciją, panaikinti ar apriboti galimybę naudotis įslaptinta informacija, sudaryti sąlygas neleistinai įslaptintą informaciją pasisavinti, paskleisti ar kitaip panaudoti.

Saugos įgaliotinis – Vyriausybinių ryšių centro prie Lietuvos Respublikos valstybės saugumo departamento (toliau vadinama – VRC) direktoriaus paskirtas VRC darbuotojas, užtikrinantis informacijos saugos reikalavimų įgyvendinimą VŠR tinkle.

VŠR tinklas – Vyriausybinio ryšio tinklas, naudojamas Vyriausybinio šifruoto ryšio (balso, fakso, duomenų perdavimo ir judriojo telefono ryšio) paslaugoms teikti.

VŠR tinklo administratorius – VRC direktoriaus paskirtas VRC darbuotojas, atliekantis techninę VŠR tinklo priežiūrą.

VŠR tinklo naudotojas – valstybės ar savivaldybės institucijos, valstybės įstaigos ar Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių, kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatyme nurodytų valstybės įmonių darbuotojas, užimantis pareigas, suteikiančias teisę naudotis VŠR tinklu, ir turintis leidimą dirbti ar susipažinti su įslaptinta informacija. VŠR tinklo naudotojas suprantamas kaip konkretus fizinis asmuo, kuris naudojasi VŠR tinklo ištekliais.

VŠR tinklo valdytojas ir tvarkytojas – VRC.

Kitos Nuostatuose vartojamos sąvokos atitinka sąvokas, nustatytas Lietuvos Respublikos įstatymuose ir kituose teisės aktuose.

4. Nuostatai parengti vadovaujantis Saugos dokumentų turinio gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. IV-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 (Žin., 2008, Nr. 127-4866), 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), Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymu (Žin. 1999, Nr. 105-3019; 2004, Nr. 4-29), Bendrosiomis įslaptintos elektroninės informacijos kriptografinės apsaugos taisyklėmis, patvirtintomis Lietuvos Respublikos paslapčių apsaugos koordinavimo komisijos 2010

m. birželio 28 d. posėdžio protokolu Nr. 56-3, Lietuvos Respublikos Vyriausybės 2005 m. gruodžio 5 d. nutarimu Nr. 1307 „Dėl įslaptintos informacijos administravimo taisyklių patvirtinimo“ (Žin., 2005, Nr. 143-5193) ir kitais teisės aktais, reglamentuojančiais įslaptintos informacijos tvarkymą.

5. Nuostatai, suderinus su Lietuvos Respublikos vidaus reikalų ministerija (toliau vadinama – VRM), tvirtinami VRC direktoriaus įsakymu.

6. Vadovaujantis šiais Nuostatais, yra parengiamos ir, suderinus su VRM, VRC direktoriaus įsakymu tvirtinamos Vyriausybinio šifruoto ryšio tinklo saugaus elektroninės informacijos tvarkymo taisyklės (toliau vadinama – Taisyklės), Vyriausybinio šifruoto ryšio tinklo veiklos tęstinumo valdymo planas (toliau vadinama – Valdymo planas) ir Vyriausybinio šifruoto ryšio tinklo naudotojų administravimo taisyklės (toliau vadinama – Administravimo taisyklės). Taisyklės, Valdymo planas ir Administravimo taisyklės yra VŠR tinklo saugos politiką įgyvendinantys dokumentai.

7. Pagal VŠR tinkle tvarkomos informacijos pobūdį VŠR tinklas priskiriamas pirmos kategorijos informacinėms sistemoms. Už VŠR tinkle tvarkomos įslaptintos informacijos saugumą atsako VŠR tinklo naudotojai.

8. VRC atlieka VŠR tinklo tvarkymo įstaigos bei VŠR tinklo valdytojo funkcijas.

9. VŠR tinklo Nuostatai yra privalomi visam VŠR tinklo personalui.

10. VŠR tinklo personalą sudaro:

10.1. saugos įgaliotinis/jo pavaduotojas (toliau vadinama – Saugos įgaliotinis);

10.2. VŠR tinklo administratorius/jo pavaduotojas (toliau vadinama – Administratorius);

10.3. VŠR tinklo naudotojai;

10.4. kiti VRC darbuotojai, užtikrinantys techninį VŠR tinklo funkcionavimą.

11. Lietuvos Respublikos institucijų ir jose esančių pareigybių, kurias užimantiems tų institucijų darbuotojams suteikiama teisė naudotis VŠR tinklu, sąrašas (toliau vadinama – Sąrašas) tvirtinamas teisės aktų nustatyta tvarka VRC teikimu.

12. VRC direktorius įsakymu skiria Administratorių ir Saugos įgaliotinį bei jų pavaduotojus, nurodo VRC padalinius/darbuotojus, užtikrinančius techninį VŠR tinklo funkcionavimą.

13. VŠR tinklo valdytojo ir tvarkytojo funkcijos ir atsakomybė:

13.1. vadovauja norminių aktų, susijusių su VŠR tinklo valdymu ir tvarkymu, priėmimui;

13.2. vadovauja ir organizuoja VŠR tinklo veiklą, skirdamas Saugos įgaliotinį, Administratorių, jų pavaduotojus ir kitus darbuotojus bei nurodo VRC padalinius, užtikrinančius techninį VŠR tinklo funkcionavimą;

13.3. kontroliuoja, kad VŠR tinklas būtų tvarkomas vadovaujantis VRC nuostatais, VŠR tinklo Nuostatais, VŠR tinklo saugos politiką įgyvendinančiais dokumentais bei kitais teisės aktais.

14. Saugos įgaliotinio, užtikrinančio VŠR tinkle tvarkomos informacijos saugą, funkcijos ir atsakomybė:

14.1. teikia VRC direktoriui pasiūlymus dėl:

14.1.1. Administratoriaus paskyrimo (Saugos įgaliotinis negali atlikti Administratoriaus funkcijų),

14.1.2. Nuostatų, Taisyklių, Valdymo plano ir Administravimo taisyklių (toliau vadinama – Saugos dokumentai) priėmimo, keitimo/papildymo ar panaikinimo,

14.1.3. saugos reikalavimų atitikties patikrinimo ir vertinimo atlikimo;

14.2. koordinuoja įslaptintos informacijos saugos incidentų tyrimą;

14.3. supažindina Administratorių, VŠR tinklo naudotojus, kitus VRC darbuotojus, užtikrinančius techninį VŠR tinklo funkcionavimą su Saugos dokumentais bei su atsakomybe už šių reikalavimų nesilaikymą;

14.4. organizuoja VŠR tinklo naudotojų apmokymus, susijusius su VŠR tinklo naudojama technine bei programine įranga;

14.5. atsako už VŠR tinklo saugos politikos įgyvendinimo organizavimą;

14.6. atsako už VŠR tinklo saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams;

14.7. atlieka kitas VRC direktoriaus pavestas ir/ar skirtas funkcijas;

14.8. Saugos įgaliotiniui nesant (liga, atostogos, komandiruotė ir pan.), laikinai jo funkcijas vykdo Saugos įgaliotinio pavaduotojas;

14.9. teikia Administratoriui ir kitiems VRC darbuotojams, užtikrinantiems techninį VŠR tinklo funkcionavimą, privalomus vykdyti nurodymus ir pavedimus.

15. Administratoriaus funkcijos ir atsakomybė:

15.1. atsako už VŠR tinklo funkcionavimą;

15.2. apmoko VŠR tinklo naudotojus naudotis VŠR tinklu;

15.3. įvertina VŠR tinklo naudotojų pasirengimą dirbti su VŠR tinklo įranga;

15.4. rengia pasiūlymus VŠR tinklo plėtimo, palaikymo, priežiūros ir duomenų saugos klausimais;

15.5. atlieka VŠR tinklo elementų (telefono, fakso aparatų, kompiuterių, telekomunikacinių tinklų) administravimą, pažeidžiamų vietų ir saugos reikalavimų atitikties nustatymą, žymi VŠR tinklo elementus lipdukais, nurodančiais aukščiausią leistiną tinkle perduodamos informacijos slaptumo žymą – „Riboto naudojimo“;

15.6. registruoja ir informuoja saugos įgaliotinį apie įslaptintos informacijos saugos incidentus ir teikia pasiūlymus jų pasekmių likvidavimui;

15.7. koordinuoja VRC padalinių/darbuotojų, užtikrinančių techninį VŠR tinklo funkcionavimą, veiklą;

15.8. Administratoriui nesant (liga, atostogos, komandiruotė ir pan.) laikinai jo funkcijas vykdo Administratoriaus pavaduotojas.

16. Pagrindinės VŠR tinklo įslaptintos informacijos saugumo užtikrinimo kryptys:

16.1. VŠR tinklu perduodamos įslaptintos informacijos šifravimas;

16.2. VŠR tinklo naudotojų skaičiaus ribojimas;

16.3. VŠR tinklo veiklą užtikrinančių VRC padalinių skyrimas;

16.4. VŠR tinkle naudojamų kabelių pažeidimo signalizacijos naudojimas;

16.5. abonentinių linijų paskirstymo dėžučių, paskirstymo spintų, esančių už saugomų zonų ribų, atidarymo signalizacija;

16.6. VŠR tinklo komutacinės dalies elektrinio maitinimo automatinis rezervavimas;

16.7. VŠR tinklo komutacinės dalies fizinė apsauga;

16.8. Vilniuje esančių telefono aparatų būklės kontrolė;

16.9. telefono aparatų ir šifravimo raktų apskaita ir apsauga;

16.10. VŠR tinklo plėtimo ir tinklui priklausančių kabelių remonto darbų atlikimas VRC jėgomis.

17. Įslaptintos informacijos sauga VŠR tinkle užtikrinama vadovaujantis:

17.1. Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymu;

17.2. Lietuvos Respublikos paslapčių apsaugos koordinavimo komisijos 2010 m. birželio 28 d. posėdžio protokolu Nr. 56-3 patvirtintomis Bendrosiomis įslaptintos elektroninės informacijos kriptografinės apsaugos taisyklėmis;

17.3. VRC direktoriaus 2010 m. birželio 30 d. įsakymu Nr. 2-8RN patvirtintu Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ar kuriais perduodama įslaptinta informacija, telekomunikacijų apsaugos reikalavimų aprašu;

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. kitais Lietuvos Respublikos, Europos Sąjungos bei NATO norminiais dokumentais, reglamentuojančiais įslaptintos informacijos apsaugą, teisės aktais.

II. INFORMACIJOS SAUGOS VALDYMAS

18. Saugos įgaliotinis, atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, kartą per du metus atlieka VŠR tinklo rizikos įvertinimą. Prireikus saugos įgaliotinis gali atlikti neeilinį rizikos įvertinimą.

19. VŠR tinklo rizikos įvertinimas išdėstomas rizikos įvertinimo ataskaitoje (Nuostatų priedas). Ji rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos VŠR tinklu perduodamos informacijos saugumui. Svarbiausi rizikos veiksniai yra šie:

19.1. subjektyvūs netyčiniai (kabelinio tinklo veiklos sutrikimai, įrangos gedimai, neteisingas veikimas, klaidingi VŠR tinklo naudotojų veiksmai ir kt.);

19.2. subjektyvūs tyčiniai (elektroninis šnipinėjimas, saugumo pažeidimai, vagystės ir kt.);

19.3. atsitiktinės aplinkybės (audros, gaisrai, vandens poveikis, elektros instaliacijos gedimas ir kt.).

20. Prireikus VRC direktorius, atsižvelgdamas į rizikos įvertinimo ataskaitą, tvirtina Rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

21. Siekdamas užtikrinti Saugos dokumentų ir kitų saugos politiką reglamentuojančių dokumentų reikalavimų įgyvendinimo organizavimą ir vykdymo kontrolę, Saugos įgaliotinis ne rečiau kaip kartą per du metus organizuoja VŠR tinklo saugos atitikties vertinimą, kurio metu:

21.1. įvertinama realios VŠR tinklo saugos situacijos atitiktis Saugos dokumentų reikalavimams;

21.2. inventorizuojama VŠR tinklo techninė ir programinė įranga;

21.3. patikrinama visose Lietuvoje įrengtose VŠR tinklo darbo vietose esanti įranga ir, esant galimybei, užsienyje esančių VŠR tinklo darbo vietų įranga;

21.4. peržiūrima ir vertinama VŠR tinklo personalui suteiktų teisių atitiktis jų vykdomoms funkcijoms;

21.5. įvertinamas pasirengimas užtikrinti VŠR tinklo veiklos tęstinumą įvykus saugos incidentui;

21.6. atliekamas rizikos įvertinimas ir koreguojama rizikos įvertinimo ataskaita.

22. Atlikus VŠR tinklo saugos atitikties vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminus VRC direktorius.

23. Techninės ir organizacinės VŠR tinkle tvarkomos informacijos saugos užtikrinimo priemonės pasirenkamos taip, kad VŠR tinklo veiklos tęstinumas ir saugus VŠR tinklo naudotojų darbas būtų užtikrinamas patiriant kuo mažiau išlaidų.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI BEI PRIEMONĖS

24. Siekiant užtikrinti VŠR tinkle tvarkomos informacijos saugumą, taikomos šios priemonės:

24.1. VŠR tinklo naudotojų skaičiaus ribojimas;

24.2. VŠR tinklo įrangos montavimas administracinėje ar aukštesnės klasės saugumo zonose;

24.3. perduodamos informacijos šifravimas;

24.4. naudojantis VŠR tinklo struktūrai priklausančiu kompiuteriu, taikomas VŠR tinklo naudotojų identifikavimas, kitų programų, užtikrinančių saugų kompiuterio darbą naudojimas;

24.5. VŠR tinklo reikmėms naudojamų kabelių pažeidimo signalizacijos naudojimas;

24.6. VŠR tinklo komutacinės dalies fizinė apsauga;

24.7. VŠR tinklo darbo vietose esančių telefono aparatų būklės kontrolė;

24.8. paskirstymo dėžučių, kabelių spintų atidarymo signalizacija.

25. Prie VŠR tinkle naudojamų telefono aparatų prijungus kompiuterį, skirtą įslaptintos informacijos, žymimos slaptumo žyma „Riboto naudojimo“, tvarkymui, jam taikomi VRC direktoriaus 2010 m. birželio 30 d. įsakymu Nr. 2-8RN patvirtintame Automatizuoto duomenų apdorojimo sistemų ir tinklų (toliau vadinama – ADA sistemos ir tinklai), kuriuose saugoma, apdorojama ar kuriais perduodama įslaptinta informacija, telekomunikacijų apsaugos reikalavimų apraše nustatyti reikalavimai, skirti ADA sistemų ir tinklų, kuriuose aukščiausia tvarkoma įslaptintos informacijos slaptumo žyma „Riboto naudojimo“, elementams.

26. Administratoriaus, Saugos įgaliotinio ir VRC operatoriaus telefono numeriai, elektroninio pašto adresai skelbiami Taisyklėse ir VŠR tinklo naudotojų sąraše, esančiame VRC interneto svetainės „www.vrc.lt“ skiltyje „Paslaugos“.

IV. REIKALAVIMAI PERSONALUI

27. Saugos įgaliotinis privalo išmanyti pagrindinius informacijos saugos principus, turėti atitinkamą kvalifikaciją, turėti leidimą dirbti su įslaptinta informacija, žymima slaptumo žyma „Slaptai“ ar aukštesne.

28. Saugos įgaliotinis turi:

28.1. vertinti rizikos veiksnių tikėtumus ir žalos galimybes, organizuoti ir kontroliuoti trūkumų pašalinimą;

28.2. analizuoti, vertinti Saugos dokumentų reikalavimų įgyvendinimą;

28.3. teikti siūlymus dėl Saugos dokumentų pakeitimo ar papildymo.

29. VŠR tinklo naudotojai privalo:

29.1. turėti leidimus dirbti su įslaptinta informacija, žymima slaptumo žyma „Riboto naudojimo“ arba aukštesne;

29.2. mokėti naudotis VŠR tinklo ryšio priemonėmis, skirtomis perduoti informaciją;

29.3. turėti darbo su kompiuteriu įgūdžių.

30. Administratorius privalo:

30.1. turėti leidimą dirbti su įslaptinta informacija, žymima slaptumo žyma „Slaptai“ ar aukštesne;

30.2. išmanyti darbą su telekomunikacijų įranga ir tinklais;

30.3. užtikrinti VŠR tinklo saugą Saugos dokumentų nustatyta tvarka.

31. VRC darbuotojai, užtikrinantys techninį VŠR tinklo funkcionavimą, privalo turėti leidimą dirbti ar susipažinti su įslaptinta informacija, žymima slaptumo žyma „Slaptai“ ar aukštesne.

V. SUPAŽINDINIMO SU DOKUMENTAIS PRINCIPAI

32. VŠR tinklo naudotojų supažindinimas su Saugos dokumentais vykdomas šiais atvejais:

32.1 prieš suteikiant naudotojui teisę naudotis VŠR tinklu;

32.2. pakeitus saugos dokumentus;

32.3. periodiškai, mokymų metu, ne rečiau kaip kartą per du metus.

33. Saugos įgaliotinis:

33.1. pasirašytinai supažindina VRC darbuotojus, užtikrinančius techninį VŠR tinklo funkcionavimą, su Saugos dokumentais;

33.2. teisės aktų nustatyta tvarka perduoda kiekvienam VŠR tinklo naudotojui Taisykles, kurių slaptumo žyma „Riboto naudojimo“;

33.3. Administratorių, VŠR tinklo naudotojus, kitus VRC darbuotojus, užtikrinančius techninį VŠR tinklo funkcionavimą informuoja apie atsakomybę už saugos užtikrinimo reikalavimų nesilaikymą.

VI. ATSAKOMYBĖ

34. VŠR tinklo personalas, pažeidęs Saugos dokumentų reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

VII. BAIGIAMOSIOS NUOSTATOS

35. Šie Nuostatai gali būti keičiami suderinus su VRM. Nuostatų pakeitimas tvirtinamas VRC direktoriaus įsakymu.

SUDERINTA
Lietuvos Respublikos
vidaus reikalų ministerijos
2010 m. rugsėjo 29 d. raštu Nr.1D-7371(6)