LIETUVOS RESPUBLIKOS TEISINGUMO MINISTRO
Į S A K Y M A S

DĖL TEISINGUMO MINISTRO 2011 M. SAUSIO 20 D. ĮSAKYMO NR. 1R-24 „DĖL ANTSTOLIŲ INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO

2012 m. lapkričio 22 d. Nr. 1R-291
Vilnius

P a k e i č i u Antstolių informacinės sistemos duomenų saugos nuostatus, patvirtintus Lietuvos Respublikos teisingumo ministro 2011 m. sausio 20 d. įsakymu Nr. 1R-24 „Dėl Antstolių informacinės sistemos duomenų saugos nuostatų patvirtinimo“ (Žin., 2011, Nr. 10-450), ir išdėstau juos nauja redakcija (pridedama).

L. E. TEISINGUMO MINISTRO PAREIGAS REMIGIJUS ŠIMAŠIUS

PATVIRTINTA
Lietuvos Respublikos teisingumo ministro
2011 m. sausio 20 d. įsakymu Nr. 1R-24
(Lietuvos Respublikos teisingumo ministro
2012 m. lapkričio 22 d. įsakymo Nr. 1R-291
redakcija)

ANTSTOLIŲ INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Valstybės įmonės Registrų centro tvarkomos Antstolių informacinės sistemos elektroninės informacijos saugumo tikslai yra šie:

1.1. sudaryti sąlygas saugiai pasiekti ir tvarkyti elektroninę informaciją Antstolių informacinėje sistemoje;

1.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, kokio nors kitokio neteisėto jos tvarkymo.

2. Valstybės įmonė Registrų centras (toliau – VĮ Registrų centras), siekdama užtikrinti tinkamą elektroninės informacijos saugumą, diegia informacijos saugumo vadybos sistemą, atitinkančią Lietuvos standarto LST ISO/IEC 27001:2006 reikalavimus.

3. Elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

3.1. elektroninės informacijos konfidencialumo užtikrinimas;

3.2. elektroninės informacijos vientisumo užtikrinimas;

3.3. elektroninės informacijos prieinamumo užtikrinimas;

3.4. veiklos tęstinumas;

3.5. Antstolių informacinės sistemos naudotojų mokymas;

3.6. asmens duomenų apsauga.

4. Antstolių informacinės sistemos valdytojo ir tvarkytojo pavadinimai ir adresai:

4.1. Antstolių informacinės sistemos valdytoja yra Lietuvos Respublikos teisingumo ministerija, kurios adresas – Gedimino pr. 30, Vilnius;

4.2. Antstolių informacinės sistemos tvarkytojai yra VĮ Registrų centras, kurios adresas – Vinco Kudirkos g. 18-3, Vilnius, ir asociacija Lietuvos antstolių rūmai, kurios adresas – Konstitucijos pr. 15, Vilnius.

5. Antstolių informacinės sistemos valdytojo funkcijos ir atsakomybė:

5.1. koordinuoja Antstolių informacinės sistemos tvarkytojos VĮ Registrų centro darbą, metodiškai jam vadovauja ir įstatymų nustatyta tvarka atlieka šio darbo priežiūrą;

5.2. organizuoja Antstolių informacinės sistemos duomenų saugos teisinės bazės plėtojimą ir įgyvendinimą;

5.3. prižiūri, kaip laikomasi Antstolių informacinės sistemos duomenų saugos reikalavimų;

5.4. organizuoja Antstolių informacinės sistemos naudotojams mokomuosius ir pažintinius kursus duomenų tvarkymo klausimais;

5.5. priima įsakymus dėl Antstolių informacinės sistemos saugumo užtikrinimo, tikrina, kaip jie vykdomi;

5.6. užtikrina veiksmingą ir spartų Antstolių informacinės sistemos tobulinimo planavimą;

5.7. kontroliuoja, kad racionaliai ir taupiai būtų naudojami darbo, materialiniai ir finansiniai ištekliai, skirti Antstolių informacinei sistemai tvarkyti;

5.8. atsako už tinkamą jam pavestų funkcijų vykdymą;

5.9. atsako už Antstolių informacinės sistemos informacijos tvarkymo teisėtumą ir informacijos saugą.

6. Antstolių informacinės sistemos tvarkytojos VĮ Registrų centro funkcijos ir

atsakomybė:

6.1. užtikrina Antstolių informacinės sistemos duomenų saugą ir saugų duomenų perdavimą kompiuterių tinklais (automatiniu būdu), teikia pasiūlymus Antstolių informacinės sistemos valdytojui, kaip tobulinti Antstolių informacinės sistemos duomenų saugą;

6.2. užtikrina Antstolių informacinės sistemos valdytojo priimtų teisės aktų ir rekomendacijų tinkamą įgyvendinimą;

6.3. ne rečiau kaip kartą per metus, atlikus rizikos analizę ar informacinių technologijų saugos atitikties vertinimą, organizuoja Antstolių informacinės sistemos saugos dokumentų persvarstymą (peržiūrėjimą);

6.4. teikia antstoliams metodinę ir informacinę pagalbą Antstolių informacinės sistemos saugos klausimais, apibendrina duomenų tvarkymo ar kitų su duomenimis atliekamų veiksmų praktiką ir teikia bendrą praktiką formuojančias rekomendacijas;

6.5. organizuoja Antstolių informacinės sistemos duomenų saugos priežiūros darbų atlikimą;

6.6. VĮ Registrų centro vadovas yra atsakingas už tinkamą šiuose nuostatuose nustatytų funkcijų vykdymą.

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

7.1. teikia Antstolių informacinės sistemos tvarkytojo vadovui pasiūlymus dėl:

7.1.1. Antstolių informacinės sistemos administratoriaus ar administratorių (toliau – administratorius) paskyrimo;

7.1.2. saugos dokumentų priėmimo, keitimo ar panaikinimo;

7.1.3. VĮ Registrų centro informacinių technologijų saugos reikalavimų atitikties vertinimo organizavimo;

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

7.3. teikia administratoriui privalomus vykdyti nurodymus ir pavedimus;

7.4. kasmet organizuoja Antstolių informacinės sistemos rizikos vertinimą;

7.5. prireikus organizuoja neeilinį Antstolių informacinės sistemos rizikos vertinimą;

7.6. periodiškai inicijuoja Antstolių informacinės sistemos naudotojams ir vartotojams seminarus informacijos saugos klausimais, informuoja juos apie informacijos saugos problematiką (siunčia priminimus elektroniniu paštu, rengia teminius seminarus, atmintines naujiems naudotojams ir vartotojams ir panašiai);

7.7. atlieka kitas Antstolių informacinės sistemos valdytojo ir tvarkytojo vadovų pavestas ir 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), jam priskirtas funkcijas.

8. Saugos įgaliotinis, įgyvendindamas elektroninės informacijos saugą Antstolių informacinėje sistemoje, yra atsakingas už tinkamą šiuose nuostatuose nustatytų funkcijų vykdymą.

9. Administratorius, atliekantis Antstolių informacinės sistemos priežiūrą, atlieka šias funkcijas:

9.1. vertina Antstolių informacinės sistemos naudotojų pasirengimą dirbti su Antstolių informacine sistema;

9.2. atlieka Antstolių informacinės sistemos naudotojams ir vartotojams suteiktų teisių ir priskirtų funkcijų atitikties vertinimą;

9.3. rengia ir tikrina (peržiūri) Antstolių informacinę sistemą sudarančių komponentų sąranką;

9.4. nustato Antstolių informacinės sistemos pažeidžiamas vietas;

9.5. atlieka Antstolių informacinės sistemos taikomų saugumo reikalavimų atitikties vertinimą;

9.6. informuoja saugos įgaliotinį apie saugos dokumentų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones.

10. Administratorius, vykdydamas Antstolių informacinės sistemos priežiūrą, yra atsakingas už tinkamą šių nuostatų 9 punkte nustatytų funkcijų vykdymą.

11. Saugų Antstolių informacinės sistemos duomenų tvarkymą reguliuoja:

11.1. Lietuvos Respublikos antstolių įstatymas (Žin., 2002, Nr. 53-2042; 2012, Nr. 76-3937);

11.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (Žin., 1996, Nr. 63-1479; 2008, Nr. 22-804);

11.3. Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai;

11.4. Saugos dokumentų turinio gairės, patvirtintos Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070);

11.5. Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės, patvirtintos Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymu Nr. 1V-247 (Žin., 2007, Nr. 78-3160);

11.6. Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai, patvirtinti Lietuvos Respublikos vidaus reikalų ministro 2008 m. spalio 27 d. įsakymu Nr. 1V-384 (Žin., 2008, Nr. 127-4866);

11.7. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas (Žin., 2011, Nr. 163-7739);

11.8. Lietuvos standartai LST ISO/IEC 27002:2009 ir LST ISO/IEC 27001:2006, Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo technika“ grupės standartai, reguliuojantys saugų informacinės sistemos duomenų tvarkymą;

11.9. kiti teisės aktai, reguliuojantys elektroninės informacijos saugumo politiką (toliau – saugos politika) ir duomenų tvarkymo teisėtumą, valstybės informacinių sistemų tvarkytojų veiklą ir duomenų saugos valdymą.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

12. Vadovaujantis Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairėmis, Antstolių informacinė sistema priskiriama 2 kategorijos informacinėms sistemoms.

13. Elektroninės informacijos priskyrimas atitinkamai kategorijai nustatomas įvertinus tvarkomų duomenų tipą ir įtaką Antstolių informacinės sistemos funkcionavimui atsižvelgiant į jų konfidencialumą, vientisumą ir pasiekiamumą.

14. Saugos įgaliotinis, vadovaudamasis Lietuvos standartu LST ISO/IEC 27005:2011 „Informacijos technologija. Saugumo technika. Informacijos saugumo rizikos valdymas“, kasmet organizuoja Antstolių informacinės sistemos rizikos veiksnių vertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį Antstolių informacinės sistemos rizikos veiksnių vertinimą.

15. Antstolių informacinės sistemos rizikos veiksnių vertinimas surašomas rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausi rizikos veiksniai yra šie:

15.1. subjektyvūs netyčiniai (duomenų tvarkymo klaidos ir apsirikimai, duomenų ištrynimas, klaidingas duomenų teikimas, fiziniai informacinių technologijų sutrikimai, duomenų perdavimo tinklais sutrikimai, programinės įrangos klaidos, netinkamas veikimas ir kita);

15.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis Antstolių informacinės sistemos duomenims gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

15.3. nenugalima jėga *(force majeure)*.

16. Rizikos veiksniai vertinami pagal elektroninės informacijos kategorijas, nustatant jų įtakos Antstolių informacinės sistemos elektroninės informacijos saugai laipsnius:

16.1. Ž – žemas. Duomenų pažeidimo poveikio laipsnis nėra didelis, padariniai nebus pavojingi – informacija pasiųsta kitam adresatui, įvesti netikslūs duomenys, dingo dalis informacijos, prarasta informacija po paskutinio kopijavimo, sugadinta operacinė sistema;

16.2. V – vidutinis. Duomenų pažeidimo poveikio laipsnis gali būti didelis, padariniai rimti – duomenys netikslūs ar visiškai sugadinti, duomenų bazių įrašai suklastoti ir nekorektiški, sunku rasti klaidas ir suklastotą informaciją, neveikia kompiuterinės programos ir operacinė sistema;

16.3. A – aukštas. Duomenų pažeidimo poveikio laipsnis labai didelis, padariniai rimti – duomenys visiškai sugadinti, dėl vagystės, gaisro ar užliejimo prarasti ne tik duomenys iš duomenų bazių, bet ir atsarginės kopijos, neveikia visa Antstolių informacinė sistema.

17. Rizikos vertinimo metu atliekamų darbų apimtis:

17.1. Antstolių informacinę sistemą sudarančių informacinių išteklių inventorizacija;

17.2. įtakos Antstolių informacinės sistemos veiklai vertinimas;

17.3. grėsmės ir pažeidimų analizė;

17.4. liekamosios rizikos vertinimas.

18. Atsižvelgdamas į rizikos įvertinimo ataskaitą, Antstolių 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.

19. Pagrindiniai elektroninės informacijos saugos priemonių parinkimo principai yra šie:

19.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

19.2. informacijos saugos priemonės diegimo kaina adekvati saugomos informacijos vertei;

19.3. kur galima, turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

20. Siekiant užtikrinti šiuose nuostatuose ir kituose saugos politiką reguliuojančiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, ne rečiau kaip kartą per metus organizuojamas informacinių technologijų saugos atitikties vertinimas, kurio metu:

20.1. įvertinama šių nuostatų ir kitų saugos politiką reguliuojančių teisės aktų ir realios informacijos saugos atitiktis;

20.2. inventorizuojama Antstolių informacinės sistemos techninė ir programinė įranga;

20.3. tikrinamos Antstolių informacinės sistemos tarnybinėse stotyse įdiegtos programos ir jų sąranka;

20.4. patikrinama (įvertinama) Antstolių informacinės sistemos duomenis tvarkantiems naudotojams, vartotojams ir administratoriams suteiktų teisių atitiktis vykdomoms funkcijoms;

20.5. įvertinamas pasirengimas užtikrinti Antstolių informacinės sistemos veiklos tęstinumą, įvykus saugos incidentui.

21. Atlikus šių nuostatų 20 punkte nurodytą vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato Antstolių informacinės sistemos valdytojas.

22. Antstolių informacinės sistemos informacinių technologijų saugos atitikties Lietuvos standartui LST ISO/IEC 27002:2009 vertinimą atlieka nepriklausomi specialistai.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

23. Priemonės ir metodai, kurie taikomi užtikrinant prieigą prie Antstolių informacinės sistemos, nurodant leistiną šios prieigos laiką ir būdą, konkrečiai nustatomi ir reguliuojami

Antstolių informacinės sistemos naudotojų administravimo taisyklėse.

24. Visos Antstolių informacinės sistemos tarnybinės stotys, naudotojų ir vartotojų darbo vietos turi būti apsaugotos nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.). Apsaugai naudojama programinė įranga turi atsinaujinti automatiškai ne rečiau kaip kartą per 2 valandas.

25. Naudoti programinę įrangą, nesusijusią su Antstolių informacinės sistemos tvarkytojo veikla atliekamomis funkcijomis (žaidimų, bylų siuntimo, internetinių pokalbių programų), neleidžiama.

26. Nešiojamieji kompiuteriai, tvarkant Antstolių informacinę sistemą, naudojami vadovaujantis VĮ Registrų centro direktoriaus 2011 m. lapkričio 18 d. įsakymu Nr. V-221 „Dėl Nešiojamų įrenginių saugumo patvirtinimo tvarkos ir Duomenų rezervinio kopijavimo ir laikmenų saugojimo tvarkos patvirtinimo“.

27. Antstolių informacinės sistemos naudotojų prieiga prie kitų valstybės institucijų arba žinybų kompiuterių tinklų ar interneto turi būti apsaugota užkardomis. Interneto turinys turi būti kontroliuojamas, nepraleidžiant nepageidaujamos informacijos. Už šios įrangos administravimo koordinavimą ir priežiūrą atsakingas Duomenų saugos skyriaus vedėjas.

28. Atsarginės duomenų kopijos daromos laikantis VĮ Registrų centro direktoriaus 2011 m. lapkričio 18 d. įsakyme Nr. V-221 „Dėl Nešiojamų įrenginių saugumo patvirtinimo tvarkos ir Duomenų rezervinio kopijavimo ir laikmenų saugojimo tvarkos patvirtinimo“ nustatytos tvarkos.

29. Duomenų atkūrimo iš atsarginių kopijų testavimas atliekamas ne rečiau kaip kartą per pusę metų.

IV. REIKALAVIMAI PERSONALUI

30. Antstolių informacinės sistemos naudotojai ir vartotojai privalo rūpintis tvarkomos informacijos saugumu.

31. Visi Antstolių informacinės sistemos naudotojai ir vartotojai privalo turėti darbo kompiuteriu įgūdžių.

32. Tvarkyti duomenis gali tik Antstolių informacinės sistemos naudotojai ir vartotojai, susipažinę su šiais nuostatais ir elektroninės informacijos saugos politiką reguliuojančiais saugos dokumentais ir raštu sutikę laikytis šių teisės aktų reikalavimų.

33. Antstolių informacinės sistemos naudotojai ir vartotojai, pažeidę šių nuostatų ar kitų saugos politiką reguliuojančių teisės aktų reikalavimus, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

34. Saugos įgaliotinis privalo išmanyti informacijos saugos užtikrinimo principus, savo darbe vadovautis 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), kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais.

35. 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.

V. ANTSTOLIŲ INFORMACINĖS SISTEMOS NAUDOTOJŲ IR VARTOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

36. Už Antstolių informacinės sistemos naudotojų ir vartotojų supažindinimo su šiais nuostatais, kitais saugos politiką reguliuojančiais teisės aktais ir atsakomybe už šių reikalavimų nesilaikymą organizavimą yra atsakingas saugos įgaliotinis.

37. Šie nuostatai ir kiti saugos politiką reguliuojantys teisės aktai skelbiami Antstolių informacinės sistemos naudotojams ir vartotojams pasiekiamame tinklalapyje. Apie svarbius

šių nuostatų ir kitų saugos politiką reguliuojančių teisės aktų pakeitimus naudotojai ir vartotojai informuojami el. paštu.

38. Antstolių informacinės sistemos naudotojai ir vartotojai su šiais nuostatais ir kitais saugos politiką reguliuojančiais teisės aktais ir atsakomybe už šių reikalavimų nesilaikymą supažindinami pasirašytinai.

39. Pakartotinai su saugos politiką reguliuojančiais teisės aktais Antstolių informacinės sistemos naudotojai ir vartotojai supažindinami tik iš esmės pasikeitus informacinėms sistemoms arba informacijos saugą reguliuojantiems teisės aktams. Informacija apie pasikeitimus saugos politiką reguliuojančiuose teisės aktuose siunčiama elektroniniu būdu.

40. Saugos įgaliotinis tvarko Antstolių informacinės sistemos naudotojų (VĮ Registrų centro darbuotojų) supažindinimo su saugos politiką reguliuojančiais teisės aktais žurnalą, kuriame pildomos šios skiltys: supažindinimo data, Antstolių informacinės sistemos naudotojo vardas, pavardė, pareigos ir parašas.

VI. BAIGIAMOSIOS NUOSTATOS

41. Antstolių informacinės sistemos valdytojas šiuos nuostatus gali keisti, pripažinti netekusiais galios savo arba saugos įgaliotinio iniciatyva.

42. Antstolių informacinės sistemos tvarkytojas VĮ Registrų centras saugos dokumentus turi persvarstyti (peržiūrėti) ne rečiau kaip kartą per kalendorinius metus. Saugos dokumentai turi būti persvarstomi (peržiūrimi) atlikus rizikos analizę ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems Antstolių informacinės sistemos tvarkytojo pokyčiams. Prireikus saugos dokumentai turi būti tikslinami ir derinami su Lietuvos Respublikos vidaus reikalų ministerija.

43. Reorganizuojant arba likviduojant Antstolių informacinę sistemą, jų elektroninė informacija turi būti saugiai perduodama kitam Antstolių informacinės sistemos valdytojui, valstybės archyvams Lietuvos Respublikos dokumentų ir archyvų įstatymo (Žin., 1995, Nr. 107-2389; 2004, Nr. 57-1982) nustatyta tvarka arba sunaikinama.

_____