LIETUVOS RESPUBLIKOS VYRIAUSIOJO VALSTYBINIO DARBO INSPEKTORIAUS

Į S A K Y M A S

DĖL POTENCIALIAI PAVOJINGŲ ĮRENGINIŲ VALSTYBĖS REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2010 m. liepos 14 d. Nr. V-227
Vilnius

Vadovaudamasis 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 ir 8 punktais, Potencialiai pavojingų įrenginių valstybės registro nuostatų, patvirtintų Lietuvos Respublikos Vyriausybės 2002 m. gegužės 9 d. nutarimu Nr. 645 (Žin., 2002, Nr. 48-1844; 2006, Nr. 10-358), 46 punktu ir atsižvelgdamas į Saugos dokumentų turinio gaires, patvirtintas Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070):

1. T v i r t i n u Potencialiai pavojingų įrenginių valstybės registro (toliau – Registras) duomenų saugos nuostatus (pridedama).

2. Neskelbiama.

3. P r i p a ž į s t u netekusiu galios Lietuvos Respublikos vyriausiojo valstybinio darbo inspektoriaus 2006 m. rugpjūčio 1 d. įsakymą Nr. 1-180 „Dėl Potencialiai pavojingų įrenginių valstybės registro duomenų saugos nuostatų patvirtinimo“ (Žin., 2006, Nr. 87-3439).

4. Neskelbiama.

5. Neskelbiama.

VYRIAUSIASIS VALSTYBINIS DARBO INSPEKTORIUS MINDAUGAS PLUKTAS

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2010 m. birželio 30 d. raštu Nr. 1D-5293

PATVIRTINTA
Lietuvos Respublikos
vyriausiojo valstybinio darbo inspektoriaus
2010 m. liepos 14 d. įsakymu Nr. V-227

POTENCIALIAI PAVOJINGŲ ĮRENGINIŲ VALSTYBĖS REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Potencialiai pavojingų įrenginių valstybės registro duomenų saugos nuostatų (toliau – Saugos nuostatai) tikslas – apibrėžti saugų Potencialiai pavojingų įrenginių valstybės registro (toliau – Registras) duomenų tvarkymą automatiniu būdu.

2. Saugos nuostatai reglamentuoja Registro elektroninės informacijos saugos valdymą, organizacinius ir techninius reikalavimus, reikalavimus personalui, dirbančiam su Registru, Registro naudotojų supažindinimo su saugos dokumentais principus.

3. Saugos nuostatai yra privalomi visiems Registro naudotojams (toliau – naudotojai), įskaitant Registro saugos įgaliotinį (toliau – saugos įgaliotinis) ir Registro administratorių (toliau – administratorius).

4. 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), 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 bei Lietuvos ir tarptautiniuose „Informacijos technologija. Saugumo metodai“ grupės standartuose, apibūdinančiuose saugų elektroninės informacijos tvarkymą, vartojamas sąvokas.

5. Saugos nuostatai nustato Registro duomenų saugos politiką (toliau vadinama – Saugos politika).

6. Registro duomenų saugos tikslai:

6.1. informacijos vientisumo, konfidencialumo ir prieinamumo užtikrinimas;

6.2. kompiuterizuotų darbo vietų reikiamo saugos lygio įdiegimas ir palaikymas;

6.3. nuolatinis vietinio kompiuterių tinklo funkcionavimo užtikrinimas bei saugos stebėsena;

6.4. tinkamo kompiuterinės, programinės ir ryšių įrangos funkcionavimo užtikrinimas;

6.5. kompiuterinio ryšio priimant ir perduodant informaciją elektroniniu būdu patikimumo ir saugos užtikrinimas.

7. Duomenų saugos užtikrinimo prioritetinės kryptys:

7.1. fizinė, techninė ir programinė (patalpų, serverių ir vietinio tinklo, naudotojų kompiuterinės technikos, programinės įrangos, duomenų) apsauga;

7.2. organizacinių saugaus darbo su informacija (ir duomenimis) priemonių įgyvendinimas ir kontrolė.

8. Registro vadovaujančioji ir tvarkymo įstaiga yra Lietuvos Respublikos valstybinė darbo inspekcija, adresas – Algirdo g. 19, LT- 03607 Vilnius (toliau – Registro tvarkymo įstaiga).

9. Už Registro duomenų saugą ir duomenų tvarkymo teisėtumą atsako Registro tvarkymo įstaiga.

10. Saugos įgaliotinis, įgyvendindamas Registro elektroninės informacijos saugą, atlieka šias funkcijas:

10.1. teikia Registro tvarkymo įstaigos vadovui pasiūlymus dėl:

10.1.1. administratoriaus paskyrimo; kai yra skiriami keli administratoriai ar administratorių grupė, turi būti aiškiai išdėstomos kiekvieno administratoriaus funkcijos ir

vienam iš jų turi būti pavedama koordinuoti bei prižiūrėti kitų administratorių veiklą;

10.1.2. saugos dokumentų priėmimo, keitimo ar panaikinimo;

10.1.3. saugos reikalavimų atitikties vertinimo atlikimo;

10.2. koordinuoja elektroninės informacijos saugos incidentų, įvykusių Registre, tyrimą;

10.3. teikia administratoriui privalomus vykdyti nurodymus bei pavedimus;

10.4. konsultuoja naudotojus saugaus duomenų tvarkymo klausimais;

10.5. inicijuoja naudotojų mokymą duomenų saugos klausimais, informuoja juos apie informacijos saugos problematiką;

10.6. kasmet organizuoja Registro rizikos įvertinimą;

10.7. įgyvendina Registro elektroninės informacijos saugą ir atsako už saugos dokumentų reikalavimų vykdymą;

10.8. atlieka kitas saugos dokumentais pavestas ir šiais Saugos nuostatais jam priskirtas funkcijas.

11. Administratorius:

11.1. diegia ir prižiūri Registro programinę įrangą;

11.2. darbuotojams suteikia teisę naudotis duomenimis priskirtoms funkcijoms atlikti;

11.3. atlieka Registrą sudarančių komponentų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, duomenų perdavimo tinklų) administravimą, pažeidžiamų vietų ir saugos reikalavimų atitikties nustatymą;

11.4. įvertina, ar naudotojai yra pasirengę darbui;

11.5. atsako už kompiuterių tinklo funkcionavimą;

11.6. daro Registro duomenų bazės atsargines duomenų kopijas;

11.7. informuoja saugos įgaliotinį apie saugos incidentus;

11.8. teikia pasiūlymus dėl duomenų saugos organizavimo.

12. Administratorius turi teisę patikrinti (peržiūrėti) Registro sąranką ir Registro būsenos rodiklius.

13. Tvarkant Registro duomenis ir užtikrinant jų saugą vadovaujamasi šiais teisės aktais:

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

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

13.3. 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);

13.4. Potencialiai pavojingų įrenginių valstybės registro nuostatais, patvirtintais Lietuvos Respublikos Vyriausybės 2002 m. gegužės 9 d. nutarimu Nr. 645 (Žin., 2002, Nr. 48-1844; 2006, Nr. 10-358);

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

13.6. Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairėmis ir Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymu Nr. 1V-247 (Žin., 2007, Nr. 78-3160; 2008, Nr. 127-4866);

13.7. 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);

13.8. šiais Saugos nuostatais ir kitais teisės aktais, reglamentuojančiais elektroninės informacijos bei duomenų saugą, Registro duomenų tvarkymą.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

14. Registras pagal jame tvarkomos elektroninės informacijos svarbą yra priskiriamas antrajai kategorijai, vadovaujantis Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymu Nr. 1V-247.

15. Registro informacijos sauga šiuose Saugos nuostatuose suprantama kaip administracinių techninių ir programinių priemonių visuma, skirta užtikrinti duomenų:

15.1. konfidencialumą, siekiant, kad su Registre tvarkomais duomenimis galėtų susipažinti tik Registro vadovaujančiosios tvarkymo įstaigos vadovo įgalioti asmenys;

15.2. vientisumą, siekiant, kad duomenys nebūtų atsitiktiniu ar neteisėtu būdu pakeisti ar sunaikinti; prieinamumą, siekiant, kad duomenys galėtų būti tvarkomi reikiamu metu.

16. Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja Registro rizikos įvertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį rizikos įvertinimą. Registro tvarkymo įstaiga kartą per kalendorinius metus, jei teisės aktai nenustato kitaip, išleidžia įsakymą dėl Registro rizikos įvertinimo. Šiame įsakyme nurodomas pagrindas rizikos įvertinimui atlikti, skiriami asmenys (ar sudaroma darbo grupė arba kviečiamas išorinis vertintojas) rizikos įvertinimo ataskaitai parengti, nustatomas rizikos įvertinimo atlikimo terminas ir apimtis. Nustatant apimtį, būtina atsižvelgti į visus rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Rizikos veiksnių Registro duomenims, techninei, programinei įrangai, registravimo dokumentams, patalpoms tikėtinumui vertinti naudojama penkiabalė rizikos veiksnių tikėtinumo ir žalos vertinimo metodika:

16.1. nereikšmingas rizikos veiksnių tikėtinumas, žala – 1 balas;

16.2. mažas rizikos veiksnių tikėtinumas, žala – 2 balai;

16.3. vidutinis rizikos veiksnių tikėtinumas, žala – 3 balai;

16.4. didelis rizikos veiksnių tikėtinumas, žala – 4 balai;

16.5. labai didelis rizikos veiksnių tikėtinumas, žala – 5 balai.

17. Saugos priemonės parenkamos, siekiant užtikrinti Registro veiklos tęstinumą, patiriant kuo mažiau išlaidų ir užtikrinant saugų Registro darbą.

18. Registro rizikos įvertinimas išdėstomas rizikos įvertinimo ataskaitoje, kuri rengiama atsižvelgiant į Saugaus elektroninės informacijos tvarkymo taisyklėse numatytus rizikos veiksnius, galinčius turėti įtaką informacijos saugai. Rengėjų pasirašyta rizikos vertinimo ataskaita yra pateikiama Registro tvarkymo įstaigos vadovui – Lietuvos Respublikos vyriausiajam valstybiniam darbo inspektoriui, kuris prireikus, atsižvelgdamas į ataskaitoje numatytas būtinas priemones, tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą ir jame nustato techninių, administracinių ir (ar) kitų išteklių poreikį, aprūpinimą ir įdiegimą rizikos valdymo priemonėms įgyvendinti.

19. Saugos įgaliotinis, siekdamas užtikrinti Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose išdėstytų nuostatų įgyvendinimą ir saugos politikos laikymosi kontrolę, kasmet organizuoja Registro informacinių technologijų saugos atitikties vertinimą, kurio metu atliekamos Registro tvarkymo įstaigos vadovo nustatytos užduotys:

19.1. įvertinti saugos dokumentų ir realios informacijos saugos situacijos atitiktį;

19.2. inventorizuoti Registro techninę ir programinę įrangą;

19.3. patikrinti ne mažiau kaip 10 procentų atsitiktinai parinktų naudotojų kompiuterinių darbo vietų, visose tarnybinėse stotyse įdiegtas programas ir jų sąranką;

19.4. patikrinti (įvertinti) naudotojams suteiktų teisių ir vykdomų funkcijų atitiktį;

19.5. įvertinti pasirengimą užtikrinti Registro veiklos tęstinumą įvykus saugos incidentui.

20. Atlikus Registro informacinių technologijų saugos atitikties vertinimą, saugos įgaliotinis parengia pastebėtų trūkumų šalinimo planą, kurį tvirtina, atsakingus vykdytojus

paskiria ir įgyvendinimo terminus nustato Registro tvarkymo įstaigos vadovas.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

21. Prieigos prie Registro užtikrinimo metodai ir priemonės:

21.1. teisė dirbti su konkrečia elektronine informacija suteikiama konkrečiam naudotojui arba naudotojų grupei;

21.2. nutraukus darbo santykius, naudotojo teisė naudotis Registru turi būti panaikinta. Naudotojui teisė dirbti su konkrečia elektronine informacija turi būti ribojama ar sustabdoma, kai vyksta naudotojo veiklos tyrimas, naudotojas yra ilgalaikėse atostogose arba perkeliamas į kitas pareigas ir keičiasi pareigybės aprašyme nurodytos ar atliekamos funkcijos;

21.3. naudotojas turi imtis priemonių, kad su Registro duomenimis negalėtų susipažinti pašaliniai asmenys;

21.4. leistinas prie Registro laikas naudotojams nėra ribojamas.

22. Reikalavimai naudojamai programinei įrangai, skirtai apsaugoti Registrą nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.):

22.1. kompiuterinėse darbo vietose turi būti naudojamos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės, kurios turi būti reguliariai atnaujinamos automatiniu būdu;

22.2. kenksmingos programinės įrangos aptikimo priemonės privalo nuolat ieškoti ir blokuoti kenksmingas programas, veikiančias sisteminiuose kataloguose esančiose rinkmenose (įskaitant suspaustas rinkmenas) serveryje ir visuose kompiuterių tinklo kompiuteriuose;

22.3. kenksmingos programinės įrangos aptikimo priemonės turi turėti apsaugos mechanizmus, blokuojančius bandymus panaikinti apsaugas.

23. Programinės įrangos naudojimo nuostatos, ribojančios programinės įrangos, nesusijusios su Registro tvarkymo įstaigos veikla ar naudotojo funkcijomis (žaidimai, bylų siuntimo, internetinių pokalbių programos ir kt.), naudojimą:

23.1. naudotojams leidžiama naudoti tik teisėtą programinę įrangą;

23.2. draudžiama naudoti programinę įrangą, nesusijusią su Registro tvarkymo įstaigos veikla;

23.3. periodiškai, ne rečiau kaip kartą per metus, turi būti tikrinama, ar nenaudojama neteisėta ir neleistina programinė įranga; radus tokią programinę įrangą, turi būti tiriami incidentai ir tokia programinė įranga turi būti pašalinama;

23.4. vidinis (žinybinis) Registro tvarkymo įstaigos kompiuterių tinklas nuo viešųjų informacijos perdavimo tinklų turi būti atskirtas užkarda (ugniasiene);

23.5. turi būti įdiegta galimybė nustatyti asmenis, kurie naudojosi prieiga prie Registro duomenų, fiksuoti jų atliktus veiksmus ir juos kaupti;

23.6. turi būti įdiegta galimybė visas užklausas į Registro duomenų bazę fiksuoti programiniu būdu;

23.7. naudotojų prieiga prie Registro duomenų leidžiama tik per registravimosi ir slaptažodžių sistemą;

23.8. administratorius savo tapatybę turi patvirtinti slaptažodžiu, kuriam keliami aukštesni reikalavimai negu naudotojų slaptažodžiams;

23.9. naudotojų prieigos valdymas apibrėžtas Registro naudotojų administravimo taisyklėse;

23.10. naudotojų instrukcijos ir saugos dokumentai turi būti prieinami naudotojams.

24. Leistinos nešiojamųjų kompiuterių naudojimo ribos:

24.1. nešiojamieji kompiuteriai Registro duomenų kaupimui neturi būti naudojami;

24.2. nešiojamieji kompiuteriai gali būti naudojami tik suvestiniams (viešiems) Registro duomenims saugoti;

24.3. nešiojamieji kompiuteriai prie Registro kompiuterių tinklo gali būti prijungiami ir

iš Registro tvarkymo patalpų išnešami tik su Registro tvarkymo įstaigos vadovo įgaliotųjų asmenų leidimu;

25. Viešaisiais telekomunikaciniais tinklais perduodamos elektroninės informacijos konfidencialumo užtikrinimui naudojamas Saugus valstybinis duomenų perdavimo kompiuterinis tinklas.

26. Metodai, kurie leidžiami užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą (nurodant nuotolinio prisijungimo prie Registro būdą, protokolą, duomenų keitimosi formatus, šifravimo, duomenų kopijų skaičiaus reikalavimus, reikalavimą teikti ir (ar) gauti duomenis automatiniu būdu tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas ir t. t.):

26.1. duomenys teikiami, naudojant Saugų valstybinį duomenų perdavimo tinklą. Registro elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų telekomunikacinių tinklų naudojant užkardą ar kitas priemones;

26.2. viešaisiais telekomunikaciniais tinklais perduodamų duomenų konfidencialumas turi būti užtikrintas, naudojant šifravimą, skirtines linijas, saugų valstybinį duomenų perdavimo tinklą ir (ar) kitas priemones;

26.3. duomenų siuntėjas ir gavėjas turi būti identifikuojami ir nustatomas jų tapatumas;

26.4. turi būti numatyta tinklo keitimo (plėtimo) tvarka ir jos laikomasi.

27. Registro fizinę saugą užtikrina šios saugos priemonės: įėjimo kontrolės sistema, stebėjimas vaizdo kamera, priešgaisrinė signalizacija ir kt.

28. Registrui administruoti naudojamas operacines sistemas, techninę ir programinę įrangą, reikalingą naudotojų funkcijoms vykdyti, diegia ir prižiūri tik Registro tvarkymo įstaigos vadovo įgaliotieji asmenys.

29. Registro programinės įrangos diegimas ir atnaujinimas gali būti atliekamas tik dalyvaujant administratoriui.

30. Registro programinės įrangos testavimas turi būti atliekamas, naudojant atskirą tam skirtą testavimo aplinką.

31. Prarasti, iškraipyti, sunaikinti Registro duomenys atkuriami iš Registro atsarginių duomenų kopijų. Registro duomenys turi būti kopijuojami ir saugomi taip, kad duomenų praradimo atveju visišką Registro funkcionalumą ir veiklą būtų galima atkurti per 1 valandą. Registro atsarginių duomenų kopijos daromos automatiniu būdu kiekvieną darbo dieną, esant aktyviai Registro duomenų bazei. Kopijos įrašomos į keičiamus informacijos kaupiklius (kompaktinius diskus ar magnetines juostas) ir saugomos seife, prieinamame tik administratoriui. Kopijų, iš kurių būtų galima atstatyti Registro duomenis, darymo ir saugojimo tvarka detaliai aprašyta Registro saugaus elektroninės informacijos tvarkymo taisyklėse.

32. Saugos įgaliotiniu gali būti skiriamas valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį, kuris geba įgyvendinti elektroninės informacijos saugą. Saugos įgaliotinis privalo išmanyti informacijos saugos užtikrinimo principus, savo darbe vadovautis šiais Saugos nuostatais, Informacinių technologijų saugos atitikties vertinimo metodika, kitais Lietuvos Respublikos teisės aktais, reglamentuojančiais Registro tvarkymą, turėti kvalifikaciją sugebėti prižiūrėti, kaip įgyvendinama saugos politika, taip pat turėti darbo su duomenų bazėmis, operacinėmis sistemomis, taikomosiomis programomis patirties.

IV. REIKALAVIMAI PERSONALUI

33. Administratoriumi gali būti skiriamas darbuotojas, išmanantis darbą su kompiuterių tinklais ir mokantis užtikrinti jų saugumą. Administratorius privalo būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais.

34. Administratoriaus ir saugos įgaliotinio pareigos yra nesuderinamos, negali būti skiriamas tas pats vienas asmuo, kuris kartu atliktų duomenų saugos ir administravimo funkcijas.

35. Naudotojai privalo turėti pagrindinius darbo kompiuteriu įgūdžius, būti susipažinę

su saugos dokumentais.

36. Naudotojai, pastebėję saugos dokumentų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai administratoriui, kuris apie tokius pažeidimus privalo informuoti saugos įgaliotinį. Įtaręs neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeisiančią Registro saugą (jos konfidencialumą, vientisumą ar prieinamumą), saugos įgaliotinis apie tai turi pranešti kompetentingoms institucijoms.

37. Saugos įgaliotinis periodiškai inicijuoja naudotojų mokymą informacijos saugos klausimais, įvairiais būdais informuoja juos apie informacijos saugos problematiką (priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės priimtiems naujiems darbuotojams ir panašiai).

38. Įvykus elektroninės informacijos saugos incidentui, saugos įgaliotinio, administratoriaus ir naudotojų veiksmus reglamentuoja Registro veiklos tęstinumo valdymo planas.

V. REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

39. Tvarkyti Registro duomenis gali tik įgalioti naudotojai, susipažinę su saugos dokumentais ir raštu sutikę laikytis saugos dokumentuose nustatytų reikalavimų.

40. Registro tvarkymo įstaigos naudotojų supažindinimą su saugos dokumentais ir atsakomybe už saugos dokumentuose nustatytų reikalavimų nesilaikymą pasirašytinai organizuoja saugos įgaliotinis ir įgyvendina kartu su teritorinių skyrių vedėjais. Išorinių naudotojų supažindinimo forma ir tvarka nustatoma duomenų teikimo sutartyje.

VI. BAIGIAMOSIOS NUOSTATOS

41. Saugos įgaliotinis organizuoja saugos dokumentų peržiūrėjimą ne rečiau kaip kartą per metus. Saugos dokumentai turi būti peržiūrimi po rizikos analizės ar informacinių technologijų saugos atitikties vertinimo atlikimo arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams institucijoje.

42. Saugos įgaliotinis, administratorius ir kiti naudotojai, pažeidę šių Saugos nuostatų ir kitų saugų informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako įstatymų nustatyta tvarka.

_____