



VALSTYBINIO STUDIJŲ FONDO DIREKTORIUS

Į S A K Y M A S

DĖL VALSTYBINIO STUDIJŲ FONDO DIREKTORIAUS 2010 M. RUGPJŪČIO 26 D. ĮSAKymo NR. V1-47 „DĖL STIPENDIJŲ IR FINANSINĖS PARAMOS STUDENTAMS INFORMACINĖS SISTEMOS NUOSTATŲ IR DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO

2016 m. gegužės 20 d. Nr. V1-37
Vilnius

Vadovaujantis Lietuvos Respublikos informacinių išteklių valdymo įstatymo 30 straipsnio 2 dalimi, Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“ 4 punktu bei Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ 7.1. punktu:

1. P a k e i č i u Stipendijų ir finansinės paramos studentams informacinės sistemos duomenų saugos nuostatus, patvirtintus Valstybinio studijų fondo direktoriaus 2010 m. rugpjūčio 26 d. įsakymo Nr. V1-47 „Dėl Stipendijų ir finansinės paramos studentams informacinės sistemos nuostatų ir duomenų saugos nuostatų patvirtinimo“ 2 punktu, ir išdėstau juos nauja redakcija (pridedama).

Direktorius

Ernestas Jasaitis

SUDERINTA

Lietuvos Respublikos vidaus reikalų ministerijos
2016 m. balandžio 29 d. raštu Nr. 1D-2691

STIPENDIJŲ IR FINANSINĖS PARAMOS STUDENTAMS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. SKYRIUS BENDROSIOS NUOSTATOS

1. Stipendijų ir finansinės paramos studentams informacinės sistemos duomenų saugos nuostatai (toliau – IS „Parama“ duomenų saugos nuostatai) nustato Stipendijų ir finansinės paramos studentams informacinėje sistemoje (toliau – IS „Parama“) tvarkomos elektroninės informacijos saugumo užtikrinimo prioritetines kryptis ir tikslus.

2. IS „Parama“ duomenų saugos nuostatuose vartojamos sąvokos:

2.1. Duomenų teikėjai – Lietuvos Respublikos švietimo ir mokslo ministerija (Studentų registras); Lietuvos Respublikos socialinės apsaugos ir darbo ministerija (Socialinės paramos šeimai informacinė sistema (toliau – SPIS)); Neįgalumo ir darbingumo nustatymo tarnyba prie Socialinės apsaugos ir darbo ministerijos (toliau – NDNT); Gyventojų registro tarnyba; kitos valstybinės institucijos ir įstaigos, nuolat teikiančios duomenis iš kitų informacinių sistemų, valstybės ir (ar) žinybinių registrų.

2.2. Duomenų teikėjai – pretenduojantys gauti finansinę paramą asmenys, paramos gavėjai, lėšų gražintojai; mokslo ir studijų institucijos; lietuvių bendruomenės užsienyje, teikiančios informaciją apie besikreipiančių asmenų lietuvišką kilmę, kiti juridiniai ir (ar) fiziniai asmenys;

2.3. Duomenų gavėjai – mokslo ir studijų institucijos; Lietuvos Respublikos švietimo ir mokslo ministerija (Studentų registras); Lietuvos Respublikos socialinės apsaugos ir darbo ministerija (SPIS); kiti juridiniai ir (ar) fiziniai asmenys, turintys įstatymų nustatytą teisę gauti duomenis ir pateikę prašymus, IS „Parama“ valdytojo nustatyta tvarka.

2.4. IS „Parama“ naudotojas – IS „Parama“ duomenų gavėjas, duomenų teikėjas, duomenų šaltinis arba IS „Parama“ tvarkytojo darbuotojas, kuris turi teisę naudotis IS „Parama“ ištekliais numatytoms funkcijoms atlikti. Jeigu toliau tekste IS „Parama“ naudotojams keliami konkretūs reikalavimai dėl IS „Parama“ duomenų saugos veiksmų, tai IS „Parama“ naudotojas suprantamas kaip konkretus fizinis asmuo, kuris naudojasi IS „Parama“ ištekliais.

2.5. Kitos IS „Parama“ duomenų saugos nuostatuose vartojamos sąvokos atitinka sąvokas, nustatytas Lietuvos Respublikos įstatymuose ir kituose teisės aktuose bei Lietuvos standartuose LST ISO/IEC 27002:2014 ir LST ISO/IEC 27001:2013.

3. Pagrindinės IS „Parama“ elektroninės informacijos saugumo užtikrinimo kryptys:

3.1. veiksmų su IS „Parama“ esančia elektronine informacija automatinis stebėjimas ir įrašų kaupimas;

3.2. fizinė elektroninės informacijos apdorojimo priemonių (Fondo patalpos, tarnybinės stotys, elektroninės informacijos perdavimo įranga, programinė įranga) apsauga;

3.3. organizacinių saugaus darbo su duomenimis priemonių įgyvendinimas ir kontrolė (IS „Parama“ duomenų gavėjų duomenų teikėjų, duomenų šaltinių, IS „Parama“ tvarkytojo darbuotojų teisių, įpareigojimų, atsakomybės ribų, detalių IS „Parama“ elektroninės informacijos tvarkymo ir administravimo taisyklių nustatymas).

3.4. duomenų bazių atsarginių kopijų darymas, bei saugojimas;

3.5. elektroninės informacijos saugojimas nuo žalingos programinės įrangos poveikio;

3.6. naudotojų (administratorių) kvalifikacijos kėlimas;

3.7. elektroninės informacijos integralumo užtikrinimas keičiantis su kitomis informacinėmis sistemomis;

3.8. elektroninės informacijos saugos priemonės saugančios nuo nesankcionuoto poveikio programinei, techninei įrangai ir programinės įrangos modifikavimo;

3.9. IS „Parama“ veiklos tęstinumo užtikrinimas.

4. IS „Parama“ tvarkymo įstaigos funkcijas atlieka Fondas, A. Goštauto g.12-407, LT-01108, Vilnius. Fondas taip pat atlieka IS „Parama“ valdytojo funkcijas. IS „Parama“ valdytojo ir tvarkytojo atliekamos funkcijos nurodytos IS „Parama“ nuostatuose.

5. Informacinės sistemos valdytojo funkcijos ir atsakomybė:

5.1. vadovauja norminių aktų, susijusių su IS „Parama“ valdymu ir tvarkymu, priėmimui.

5.2. vadovauja ir organizuoja IS „Parama“ veiklą, skirdamas IS „Parama“ saugos įgaliotinį, IS „Parama“ administratorių bei kitus darbuotojus

5.3. kontroliuoja, kad IS „Parama“ būtų tvarkoma vadovaujantis Fondo nuostatais, IS

5.4. „Parama“ nuostatais ir šiais IS „Parama“ duomenų saugos nuostatais bei kitais teisės aktais;

5.5. atsako už IS „Parama“ saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams.

6. Informacinės sistemos tvarkytojas (-ai) atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka.

7. Saugos įgaliotinio, įgyvendinančio IS „Parama“ elektroninės informacijos saugą, funkcijos ir atsakomybė:

7.1. teikia Informacinės sistemos valdytojui pasiūlymus dėl:

7.1.1. IS „Parama” administratorių paskyrimo (saugos įgaliotinis negali atlikti IS „Parama” administratoriaus funkcijų);

7.1.2. saugos dokumentų priėmimo, keitimo ar panaikinimo;

7.1.3. IS „Parama” informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

7.2. koordinuoja elektroninės informacijos saugos incidentų tyrimą;

7.3. teikia IS „Parama” administratoriams privalomus vykdyti nurodymus ir pavedimus;

7.4. pasirašytinai supažindina IS „Parama” tvarkytojo darbuotojus, kitus IS „Parama” naudotojus, IS „Parama” administratorius su IS „Parama” duomenų saugos nuostatais ir saugos politiką įgyvendinančiais teisės aktais bei atsakomybe už šių reikalavimų nesilaikymą;

7.5. organizuoja IS „Parama” administratorių, IS „Parama” tvarkytojo darbuotojų ir kitų IS „Parama” naudotojų kvalifikacijos tobulinimą duomenų saugos klausimais, reguliariai jiems primena saugumo problemas (elektroniniu paštu, atmintinės naujai priimtiems darbuotojams ir pan.);

7.6. atlieka kitas Informacinės sistemos valdytojo pavestas ir jam priskirtas funkcijas;

7.7. atsako už IS „Parama” saugos politikos įgyvendinimo organizavimą;

7.8. atsako už IS „Parama” saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams.

8. IS „Parama” administratoriaus funkcijos ir atsakomybė:

8.1. atsako už IS „Parama“ funkcionavimą;

8.2. įvertina IS „Parama” naudotojų pasirengimą dirbti su IS „Parama” ir suteikia jos naudotojams teisę naudotis informacinės sistemos galimybėmis paskirtoms funkcijoms atlikti;

8.3. rengia pasiūlymus IS „Parama” kūrimo, palaikymo, priežiūros ir duomenų saugos klausimais;

8.4. atlieka IS „Parama” sudarančių komponentų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, įsilaužimų aptikimo sistemų, duomenų perdavimo tinklų) administravimą, pažeidžiamų vietų ir saugos reikalavimų atitikties nustatymą;

8.5. registruoja ir informuoja saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikia pasiūlymus.

9. Duomenų sauga IS „Parama” užtikrinama vadovaujantis:

9.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

9.2. Lietuvos Respublikos kibernetinio saugumo įstatymu;

9.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

9.4. Bendraisiais elektroninės informacijos saugos reikalavimais, Saugos dokumentų turinio gairių aprašu, Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašu, patvirtintais Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

9.5. Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;

9.6. Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintais Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12);

9.7. Lietuvos standartais LST ISO/IEC 27002:2014, LST ISO/IEC 27001:2013, taip pat kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo metodai“ grupės standartais, apibūdinančiais saugų informacinės sistemos duomenų tvarkymą;

9.8. IS „Parama“ duomenų saugos nuostatais;

9.9. IS „Parama“ tvarkytojo darbo vietoms skirtomis darbo instrukcijomis, saugaus elektroninės informacijos tvarkymo taisyklėmis, naudotojų administravimo taisyklėmis, IS „Parama“ veiklos tęstinumo valdymo planu ir kitais teisės aktais, reglamentuojančiais duomenų tvarkymo teisėtumą bei duomenų saugos valdymą.

II. SKYRIUS ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

10. IS „Parama“ tvarkoma elektroninė informacija, kuri yra nurodyta IS „Parama“ nuostatuose. Šių duomenų konfidencialumo, vientisumo ir (ar) prieinamumo praradimas gali turėti neigiamą įtaką Fondo veiklai. Sutinkamai su Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairėmis IS „Parama“ priskiriama antrai informacinės sistemos kategorijai.

11. Prioritetinis IS „Parama“ duomenų pateikimo būdas yra elektroninės informacijos priemonės. Užtikrinamas pirmos kategorijos IS „Parama“ prieinamumas – ne mažiau 96 proc. laiko visą parą.

12. Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja IS „Parama“ rizikos įvertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį rizikos įvertinimą. IS „Parama“ rizikos veiksnių vertinimas atliekamas kokybiniu rizikos vertinimo metodu.

13. IS „Parama“ rizikos įvertinimas išdėstomas Rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksmus, galinčius turėti įtakos IS „Parama“ informacijos saugai. Svarbiausi rizikos veiksniai yra šie:

13.1. subjektyvūs netyčiniai (duomenų tvarkymo klaidos ir apsirikimai, duomenų ištrynimai, klaidingas duomenų teikimas, fiziniai informacijos technologijų sutrikimai, duomenų perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kt.);

13.2. subjektyvūs tyčiniai (nesankcionuotas naudojimas duomenims gauti, duomenų pakeitimas ir sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kt.);

13.3. atsitiktinės subjektyvios aplinkybės (darbuotojų praradimas, audros, gaisrai, vandens poveikis, elektros instaliacijos gedimas ir kt.).

14. Atsižvelgdamas į rizikos įvertinimo ataskaitą, Informacinės sistemos valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

15. Siekdamas užtikrinti IS „Parama“ duomenų saugos nuostatuose ir saugos politiką įgyvendinančiuose teisės aktuose nustatytų reikalavimų įgyvendinimo organizavimą ir kontrolę, saugos įgaliotinis ne rečiau kaip kartą per 1 metus organizuoja informacinių technologijų (toliau – IT) saugos atitikties vertinimą, kurio metu:

15.1. įvertinama IS „Parama“ duomenų saugos nuostatų, saugos politiką įgyvendinančių teisės aktų ir realios duomenų saugos situacijos atitiktis;

15.2. inventorizuojama IS „Parama“ techninė ir programinė įranga;

15.3. tikrinama IS „Parama“ tarnybinėse stotyse, administratorių, IS „Parama“ tvarkytojo darbuotojų kompiuterinėse darbo vietose įdiegta programinė įranga ir jos sąranka;

15.4. peržiūrima IS „Parama“ administratoriui, IS „Parama“ tvarkytojo darbuotojams, kitiems IS „Parama“ naudotojams suteiktų teisių atitiktis jų vykdomoms funkcijoms;

15.5. įvertinamas pasirengimas užtikrinti IS „Parama“ veiklos tęstinumą įvykus saugos incidentui;

15.6. atliekamas rizikos įvertinimas ir IS „Parama“ duomenų saugos nuostatuose reglamentuota tvarka koreguojama rizikos įvertinimo ataskaita.

16. Atlikus IT saugos atitikties vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminus Informacinės sistemos valdytojas (IS „Parama” tvarkymo įstaigos vadovas).

17. Techninės, programinės ir organizacinės elektroninės informacijos saugos priemonės pasirenkamos, kad būtų užtikrintas IS „Parama” veiklos tęstinumas patiriant kuo mažiau išlaidų ir saugus IS „Parama” naudotojų darbas.

III. SKYRIUS ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

18. IS „Parama” duomenų saugai yra taikomos tam tikros programinės įrangos naudojimo nuostatos:

18.1. IS „Parama” tarnybinėse stotyse, administratorių, IS „Parama” tvarkytojo darbuotojų kompiuterinėse darbo vietose įdiegta legali ir saugi programinė įranga (operacinė sistema su naujaisiais pataisymais);

18.2. IS „Parama” tarnybinių stočių, IS „Parama” tvarkytojo darbuotojų kompiuterinių darbo vietų operacinių sistemų ir taikomųjų programų sąranka parenkama tokiu būdu, kad būtų užtikrintas didžiausias saugumo lygis (išjungiami nereikalingi darbai procesai ir reikmenys (angl. services), ribojamas arba išjungiamas priėjimas prie operacinės sistemos prievadų);

18.3. IS „Parama” tarnybinėse stotyse, IS „Parama” tvarkytojo darbuotojų kompiuterinėse darbo vietose įdiegiama programinė įranga, skirta apsisaugoti nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir pan.). Programinė įranga atnaujinama kiekvieną darbo dieną. Programinę įrangą atnaujina ir kontroliuoja IS „Parama” tvarkytojo atsakingi darbuotojai.

18.4. IS „Parama“ tarnybinėse stotyse, administratorių, tvarkytojų kompiuterinėse darbo vietose turi būti naudojama tik su IS „Parama” veikla susijusi programinė įranga. Programinės įrangos diegimą atlieka tik IS „Parama” tvarkytojo atsakingi darbuotojai.

19. Kompiuterinis tinklas, prie kurio prijungtos IS „Parama” tarnybinės stotys, IS „Parama“ administratorių kompiuteriai nuo viešojo interneto yra atskirtas užkarda (angl. firewall).

20. Pagrindinė IS „Parama” duomenų pateikimo prieiga yra duomenų perdavimas duomenų perdavimo kanalu, panaudojant saugų HTTPS protokolą. IS „Parama” naudotojai identifikuojami ir jiems suteikiamos teisės informacinėje sistemoje pagal jam suteiktą identifikatorių ir atitinkamą slaptažodį. Kaip papildoma priemonė, ribojanti prisijungimą prie IS „Parama”, yra interneto protokolo (angl. IP) adresų filtravimas.

21. Kaip papildomas IS „Parama“ duomenų pateikimo būdas yra duomenų pateikimas IS „Parama“ duomenų gavėjams žodžiu, nustačius duomenų gavėjo tapatybę, pažymų ar kitų dokumentų, kurie gali būti teikiami raštu ar elektroniniu būdu, formavimas.

22. IS „Parama“ IS „Parama“ tvarkytojo darbuotojų kompiuterių prisijungimas nuotoliniu būdu prie Fondo informacinių resursų leidžiamas Informacinės sistemos valdytojo pavaduotojo leidimu, panaudojant VPN (angl. Virtual Private Network) technologiją, duomenų šifravimą bei papildomas tapatybės nustatymo galimybes.

23. Informacijos pasikeitimo būdai su kitomis organizacijomis nustatomi asmens duomenų teikimo sutartimis. Informacija elektroniniu būdu teikiama sudarytu saugiu VPN-tuneliu, kuriame naudojamas 3DES (angl. Triple Data Encryption Algorithm) šifravimo algoritmas su SHA (angl. Secure Hash Algorithm) hešavimo funkcija.

24. Dalis Fondo nustatytų IS „Parama“ naudotojų jungiasi prie Fondo WEB aplikacijos HTTPS protokolu, identifikuodami Fondo serverį jam išduotu SSL (angl. Secure Sockets Layer) sertifikatu. Kita IS „Parama“ Fondo nustatytų naudotojų dalis jungiasi prie sistemos fiziškai apsaugotomis ryšio linijomis, kurios neprieinamos iš išorės, autorizuodami save IS „Parama“ naudotojo vardu ir slaptažodžiu.

25. IS „Parama“ naudotojo vardo ir slaptažodžio apsaugojimo nuo jų atskleidimo parinkimo mechanizmas remiasi prailgintu autorizacijos laiku, kuris nuolat didėja priklausomai nuo nesėkmingų autorizacijų skaičiaus.

26. Duomenų subjektui asmens duomenys teikiami HTTPS protokolu autorizuojant duomenų subjektą per Elektroninius valdžios vartus.

27. Kopijų, iš kurių būtų galima atstatyti IS „Parama“ duomenis, darymo ir saugojimo tvarka detalčiai aprašoma IS „Parama“ saugaus elektroninės informacijos tvarkymo taisyklėse.

IV. SKYRIUS REIKALAVIMAI PERSONALUI

28. IS „Parama“ saugos įgaliotinis privalo išmanyti informacijos saugos užtikrinimo principus, savo darbe vadovautis techniniais valstybės registru (kadastru), žinybinių registru, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr.1V-832, Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais IS „Parama“ duomenų tvarkymą, standartais bei kitais dokumentais ir būti susipažinęs su esminiais reikalavimais, turėti atitinkamą kvalifikaciją, sugebėti prižiūrėti, kaip įgyvendinama saugos politika, taip pat turėti darbo su duomenų bazėmis, operacinėmis sistemomis,

taikomosiomis programomis patirties. Saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

29. IS „Parama” administratorius privalo išmanyti informacijos saugos principus, darbą su kompiuterių tinklais, mokėti užtikrinti jų saugumą, taip pat administruoti ir prižiūrėti duomenų bazes, turi būti susipažinęs su IS „Parama” duomenų saugos nuostatais ir saugos politiką įgyvendinančiais teisės aktais, taip pat kitomis vidaus ir darbo saugos taisyklėmis.

30. IS „Parama” tvarkytojo darbuotojai privalo turėti pagrindinius darbo su kompiuteriu įgūdžius, mokėti tvarkyti IS „Parama” duomenis IS „Parama” darbo instrukcijų nustatyta tvarka ir būti susipažinę su IS „Parama” nuostatais ir IS „Parama” duomenų saugos nuostatais, saugos politiką įgyvendinančiais teisės aktais.

31. IS „Parama” naudotojai, kurie naudosis IS „Parama” duomenimis, privalo turėti pagrindinius darbo su kompiuteriu įgūdžius, būti susipažinę su IS „Parama” duomenų saugos nuostatais ir saugos politiką įgyvendinančiais teisės aktais.

32. IS „Parama” IS „Parama” tvarkytojo darbuotojai ir kiti IS „Parama” naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veiklos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti IS „Parama” saugos įgaliotiniui ir/arba IS „Parama” administratoriui.

33. Esant elektroninės informacijos saugos incidentui, nenumatytai situacijai, IS „Parama” saugos įgaliotinio, IS „Parama” administratoriaus, IS „Parama” tvarkytojo darbuotojų ir kitų IS „Parama” naudotojų veiksmus reglamentuoja IS „Parama” veiklos tęstinumo valdymo planas.

34. IS „Parama” saugos įgaliotinis kartą per metus organizuoja IS „Parama” administratorių, IS „Parama” IS „Parama” tvarkytojo darbuotojų ir kitų IS „Parama” naudotojų mokymus kvalifikacijos tobulinimo ir duomenų saugos klausimais, nuolat jiems primena saugumo problemas (elektroniniu paštu, per internetinę svetainę, atmintinėmis naujai priimtiems darbuotojams ir pan.).

V. SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS
DOKUMENTAIS PRINCIPAI

35. IS „Parama” duomenis tvarkyti gali tik tie asmenys, kurie susipažinę su IS „Parama” duomenų saugos nuostatais, saugos politiką įgyvendinančiais teisės aktais, atsakomybe už saugos reikalavimų pažeidimą ir raštiškai sutikę laikytis šių teisės aktų reikalavimų.

36. IS „Parama” naudotojai saugos nuostatus ir saugos politiką įgyvendinančius teisės aktus gauna sutarties dėl duomenų teikimo pasirašymo metu.

37. IS „Parama” nuostatai ir IS „Parama” duomenų saugos nuostatai skelbiami Fondo tinklalapyje.

38. Už IS „Parama” IS „Parama” tvarkytojo darbuotojų supažindinimą su IS „Parama” duomenų saugos nuostatais ir dokumentais, įgyvendinančiais saugos politiką, atsako IS „Parama” saugos įgaliotinis.

39. IS „Parama” naudotojai, pažeidę IS „Parama” duomenų saugos nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų nuostatas, atsako įstatymų nustatyta tvarka.