LIETUVOS AUKŠTŲJŲ MOKYKLŲ ASOCIACIJOS BENDRAJAM PRIĖMIMUI ORGANIZUOTI PREZIDENTAS

ĮSAKYMAS DĖL LIETUVOS AUKŠTŲJŲ MOKYKLŲ ASOCIACIJOS BENDRAJAM PRIĖMIMUI ORGANIZUOTI PREZIDENTO 2011 M. GEGUŽĖS 20 D. ĮSAKYMO NR. 11-03 „DĖL BENDROJO PRIĖMIMO Į LIETUVOS AUKŠTĄSIAS MOKYKLAS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO" PAKEITIMO

2022 m. gegužės 5 d. Nr. 22-08
Kaunas

1. P a k e i č i u Lietuvos aukštųjų mokyklų asociacijos bendrajam priėmimui organizuoti prezidento 2011 m. gegužės 20 d. įsakymą Nr. 11-03 „Dėl bendrojo priėmimo į Lietuvos aukštąsias mokyklas informacinės sistemos duomenų saugos nuostatų patvirtinimo" ir išdėstau jį nauja redakcija:

LIETUVOS AUKŠTŲJŲ MOKYKLŲ ASOCIACIJOS BENDRAJAM PRIĖMIMUI ORGANIZUOTI PREZIDENTAS

ĮSAKYMAS DĖL BENDROJO PRIĖMIMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

Vadovaudamasis Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo" ir Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo":

T v i r t i n u Bendrojo priėmimo informacinės sistemos duomenų saugos nuostatus (pridedama);

2. Į p a r e i g o j u Bendrojo priėmimo informacinės sistemos duomenų valdymo įgaliotinę Ramunę Bakanovienę su BPIS saugos nuostatais supažindinti BPIS duomenų saugos įgaliotinį ir BPIS administratorių.

SUDERINTA
Nacionalinio kibernetinio saugumo centro
2022-05-04
Raštu Nr. (4.1E) 6K-427

Asociacijos prezidentas Pranas Žiliukas

Parengė: Ramunė Bakanovienė, tel. Nr.: 8 37 214 240 el. paštas: ramuneb@lamabpo.lt

PATVIRTINTA
LAMA BPO prezidento
2011 m. gegužės 20 d. įsakymu Nr. 11-03
(2022 m. gegužės 5 d. įsakymu Nr. 22-08
nauja redakcija)

BENDROJO PRIĖMIMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Bendrojo priėmimo informacinės sistemos (toliau – BPIS) duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato BPIS saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą.

2. Šiuose Saugos nuostatuose vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų, patvirtintų Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ apraše (toliau – Aprašas) ir Lietuvos standartuose LST ISO/IEC 27001:2013 ir LST ISO/IEC 27002:2014.

3. BPIS duomenų saugos tikslas – užtikrinti BPIS duomenų prieinamumą, vientisumą, konfidencialumą ir tinkamą kompiuterizuotų darbo vietų bei tinklo įrangos funkcionavimą.

4. BPIS duomenų saugumui užtikrinti kompleksiškai naudojamos administracinės, techninės ir programinės priemonės, padedančios įgyvendinti reagavimo, atsakomybės, elektroninės informacijos saugos suvokimo ir saugos priemonių projektavimo ir diegimo principus.

5. BPIS duomenų saugos užtikrinimo prioritetinės kryptys:

5.1. duomenų tvarkymui naudojamos techninės ir programinės įrangos kontrolė;

5.2. duomenų tvarkymo kontrolė;

5.3. naudojimosi BPIS duomenimis kontrolė.

6. Saugos nuostatų reikalavimai taikomi BPIS valdytojui ir BPIS tvarkytojui – Lietuvos aukštųjų mokyklų asociacijai bendrajam priėmimui organizuoti (toliau – LAMA BPO), įsikūrusiai adresu Studentų g. 54, 51424 Kaunas.

7. LAMA BPO tiesiogiai atsako už:

7.1. elektroninės informacijos saugą;

7.2. saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą;

7.3. reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka.

8. LAMA BPO skiria saugos įgaliotinį, kuris, koordinuodamas ir prižiūrėdamas saugos politikos įgyvendinimą, atlieka šias funkcijas:

8.1. teikia LAMA BPO vadovui pasiūlymus dėl:

8.1.1 BPIS administratoriaus paskyrimo ir reikalavimų administratoriui nustatymo;

8.1.2 LAMA BPO informacinių technologijų saugos atitikties vertinimo atlikimo Aprašo VII skyriuje nurodytoje metodikoje nustatyta tvarka;

8.1.3 saugos dokumentų priėmimo, keitimo;

8.2. koordinuoja elektroninės informacijos saugos incidentų, įvykusių informacinėje sistemoje, tyrimą ir bendradarbiauja su kompetentingoms institucijoms, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais;

8.3. teikia BPIS administratoriui ir informacinės sistemos naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;

8.4. organizuoja rizikos įvertinimą;

8.5. atlieka kitas Saugos nuostatuose, kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą, nustatytas ir Aprašo jam priskirtas funkcijas;

8.6. saugos įgaliotinis periodiškai organizuoja informacinės sistemos naudotojų mokymą elektroninės informacijos saugos klausimais, įvairiais būdais informuoja juos apie elektroninės informacijos saugos problemas.

9. LAMA BPO skiria BPIS administratorių, kuris atlieka šias funkcijas:

9.1. BPIS naudotojų teisių valdymas;

9.2. BPIS komponentų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, įsilaužimų aptikimo sistemų, elektroninės informacijos perdavimu tinklais, serverių ir kitų) sąranka;

9.3. BPIS pažeidžiamų vietų nustatymas;

9.4. saugumo reikalavimų atitikties nustatymas ir stebėsena;

9.5. reagavimas į BPIS saugos incidentus;

9.6. visų saugos įgaliotinio nurodymų ir pavedimų, susijusių su informacinės sistemos saugos užtikrinimu, vykdymu;

9.7. nuolatinės informacijos apie saugą užtikrinančių pagrindinių komponentų būklę teikimas saugos įgaliotiniui.

10. Administratorius privalo patikrinti (peržiūrėti) informacinės sistemos sąranką ir informacinės sistemos būsenos rodiklius reguliariai, ne rečiau kaip kartą per metus ir (arba) po informacinės sistemos pokyčio.

11. Teisės aktai, kuriais vadovaujamasi tvarkant elektroninę informaciją ir užtikrinant jos saugumą, sąrašas:

11.1. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas);

11.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

11.3. Lietuvos Respublikos kibernetinio saugumo įstatymas;

11.4. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

11.5. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

11.6. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, saugos dokumentų turinio gairių aprašas ir elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas, patvirtinti Lietuvos Respublikos vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl bendrųjų elektroninės informacijos saugos reikalavimų aprašo, saugos dokumentų turinio gairių aprašo ir elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“;

11.7. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti LR Krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

11.8. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta LR Krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

11.9. Lietuvos standartai LST ISO/IEC 27001:2017 ir LST ISO/IEC 27002:2017 Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, nustatantys saugų elektroninės informacijos tvarkymą;

11.10. LAMA BPO asmens duomenų tvarkymo taisyklės, patvirtintos LAMA BPO prezidento 2020 m. balandžio 20 d. įsakymu Nr. 20-03 (LAMA BPO prezidento įsakymo 2022 m. vasario 28 d. Nr. 22-04 pakeitimas);

11.11. kiti teisės aktai, reglamentuojantys duomenų tvarkymo teisėtumą ir duomenų saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

12. BPIS tvarkoma elektroninė informacija, vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, priskirtina vidutinės svarbos elektroninės informacijos kategorijai.

13. Vidutinės svarbos informacijos kategorijai priskiriama informacija, nes ji atitinka šiuos kriterijus, galinčius:

13.1. pažeisti daugiau nei 1 procento, bet ne daugiau nei 5 procentų valstybės gyventojų teises ir teisėtus interesus;

13.2. lemti, kad nebus atliekama (-os) kuri nors (kurios nors) gyvybiškai svarbi (-ios) funkcija (-os) vienam ministrui pavestoje valdymo srityje;

13.3. vienai ar kelioms institucijoms padaryti finansinių nuostolių, didesnių nei 30 000 eurų, bet ne didesnių nei 300 000 eurų.

14. BPIS priskiriama trečiosios svarbos kategorijai vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo nuostatomis ir Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais.

15. BPIS rizika vertinama vadovaujantis Rizikos analizės vadovu, skelbiamu NKSC interneto svetainėje, Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais.

16. Atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos BPIS kibernetiniam saugumui, vertinimas. BPIS rizikos įvertinimas surašomas rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai.

17. Svarbiausieji rizikos veiksniai yra šie:

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

17.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema duomenims gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

17.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840, 3 punkto nuostatose.

18. Rizikos vertinimas atliekamas kartą per metus. Jo metu vertinant riziką vykdomos šios veiklos:

18.1. BPIS sudarančių informacinių išteklių inventorizacija;

18.2. įtakos LAMA BPO vertinimas;

18.3. grėsmės ir pažeidimų analizė;

18.4. likutinės rizikos vertinimas.

19. Už rizikos vertinimo organizavimą atsakingas BPIS saugos įgaliotinis.

20. Atsižvelgdamas į rizikos įvertinimo ataskaitą, BPIS valdytojas, esant reikalui, tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą.

21. Rizikos įvertinimo ataskaitas, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas, informacinių technologijų saugos atitikties vertinimo ataskaitas, pastebėtų trūkumų šalinimo plano kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai nustatyta tvarka.

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

22.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

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

22.3. kur įmanoma, turi būti įdiegtos prevencinės, detektinės ir korekcinės informacijos saugos priemonės.

23. Informacinių technologijų saugos atitikties vertinimas atliekamas vadovaujantis Informacinių technologijų saugos atitikties vertinimo metodika ir reikalavimais.

24. Informacinių technologijų saugos atitikties vertinimas atliekamas vieną kartą per dvejus metus.

25. Atliekant informacinių technologijų saugos atitikties įvertinimą yra:

25.1. įvertinama esamos informacijos saugos situacijos atitiktis reikalavimams ir saugos politikos įgyvendinimo teisės aktų reikalavimams;

25.2. inventorizuojama BPIS techninė ir programinė įranga;

25.3. patikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų BPIS naudotojų kompiuterinių darbo vietų bei visų tarnybinių stočių programinė įranga ir jų sąranka;

25.4. įvertinama BPIS duomenis tvarkantiems naudotojams ir administratoriams suteiktų teisių atitiktis vykdomoms funkcijoms;

25.5. įvertinama pasirengimas užtikrinti BPIS veiklos tęstinumą įvykus saugos incidentui.

26. Už Informacinių technologijų saugos atitikties vertinimo organizavimą atsakingas BPIS saugos įgaliotinis.

27. Atlikus informacinių technologijų saugos atitikties įvertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama BPIS valdytojo vadovui, ir pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato BPIS valdytojo vadovas.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

28. BPIS turi atitikti Techninius valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimus, patvirtintus LR Krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“.

29. BPIS turi atitikti Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams aprašo reikalavimus, patvirtintus Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. Nr. 818 nutarimu „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

30. Programinės įrangos, įdiegtos tarnybinėse stotyse ir naudotojų kompiuteriuose, naudojimo nuostatos:

30.1. Tarnybinėse stotyse neturi veikti programinė įranga, nesusijusi su BPIS elektroninės informacijos tvarkymu, jos naudotojų ir pačios įrangos administravimu;

30.2. prieiga prie BPIS tarnybinių stočių operacinių sistemų valdymo ir konfigūravimo leidžiama tik BPIS administratoriui, atsakingam už BPIS administravimą ir priežiūrą;

30.3. programinės įrangos diegimą, šalinimą ir konfigūravimą gali atlikti tik BPIS administratorius;

30.4. BPIS programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu;

30.5. BPIS naudotojų, darbo vietose naudojama programinė įranga, skirta apsaugoti naudotojų darbo vietas nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.). Ši programinė įranga turi būti atnaujinama reguliariai, ne rečiau kaip kartą per savaitę;

30.6. tarnybinėse stotyse ir kompiuterinėse darbo vietose turi būti naudojama tik legali ir funkcionalumui užtikrinti būtina programinė įranga;

30.7. programinė įranga turi būti nuolat atnaujinama laikantis gamintojo reikalavimų;

30.8. turi būti įdiegta galimybė fiksuoti ir kaupti duomenis apie asmenų, kurie naudojasi prieiga prie BPIS elektroninės informacijos, atliktus veiksmus.

31. Kitoms institucijoms elektroniniai duomenys teikiami tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir technines sąlygas, naudojant saugų duomenų perdavimo būdą.

32. Leistinos BPIS vidinių naudotojų kompiuterių naudojimo ribos:

32.1. tarnybiniuose kompiuteriuose, planšetėse ir kituose įrenginiuose turi būti užtikrintas darbuotojo tapatybės autentifikavimas, kiekvieno prisijungimo prie kompiuterio metu įvedant vartotojo vardą ir slaptažodį;

32.2. prieiga prie tarnybinių kompiuterių, planšečių ar kitų įrenginių turi būti vykdoma naudojant VPN (Virtualus privatus tinklas), įdiegtą LAMA BPO maršrutizatoriuje ir kiekviename vartotojo įrenginyje. Duomenys, esančius nešiojamuose kompiuteriuose, planšetėse taip pat kituose įrenginiuose, šifruojami operacinės sistemos priemonėmis. Kiekvieną kartą jungiantis prie tarnybinių kompiuterių, planšečių ar kitų įrenginių ne iš LAMA BPO centrinės būstinės interneto tinklo, darbuotojas privalo aktyvuoti VPN.

33. BPIS turi būti apsaugota nuo:

33.1. neautentifikuotos prieigos;

33.2. nesankcionuoto naudotojo sesijos perėmimo;

33.3. nesankcionuoto duomenų perėmimo ar jų įterpimo;

33.4. žalingo kodo įterpimo (angl. Injection, XSS (Cross-sitescripting));

33.5. kitų saugumo pažeidimų, kurie įvardijami OWASP TOP 10 (https://www.owasp.org) sąraše (arba lygiaverčiame).

34. Programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims.

35. Apsaugai naudojama programinė įranga turi turėti apsaugos mechanizmus, blokuojančius kenkimo programų bandymus panaikinti apsaugas nuo kenkimo programų.

36. BPIS programinės įrangos kopijos turi būti daromos pagal nustatytą planą.

37. Darant atsargines kopijas programinė įranga turi informuoti el. paštu BPIS administratorių apie sėkmingai ar nesėkmingai atliktą atsarginės kopijos sukūrimą.

38. Kopijos suformavimo ir atlikimo įrašai turi būti fiksuojami ir saugomi atsarginių kopijų žurnale.

39. Atsarginės laikmenos su BPIS programinės įrangos kopijomis turi būti laikomos kitose patalpose nei yra BPIS tarnybinės stotys.

40. Ne rečiau nei kartą per metus turi būti atliktas BPIS atkūrimo bandymas iš atsarginės laikmenos su BPIS programinės įrangos kopijos.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

41. Saugos įgaliotinis turi išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis BPIS saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų duomenų tvarkymą.

42. Saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat galiojančią 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 arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

43. BPIS administratoriumi gali būti skiriamas valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo ar kitą sutartį, išmanantis darbą su kompiuterių tinklais ir mokantis užtikrinti jų saugumą. Administratorius privalo būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais. BPIS administratorius privalo turėti sisteminių programinių priemonių administravimo bei priežiūros patirties.

44. BPIS naudotojai privalo turėti saugaus darbo kompiuteriu įgūdžius.

45. Tvarkyti BPIS duomenis gali tik BPIS naudotojai, susipažinę su Saugos nuostatais ir elektroninės informacijos saugos politiką reguliuojančiais saugos dokumentais bei raštu sutikę laikytis šių teisės aktų reikalavimų. Nesutikę su šia saugos dokumentacija asmenys neturi teisės dirbti su BPIS.

46. BPIS naudotojai, pažeidę Saugos nuostatų ar kitų saugos politiką reguliuojančių teisės aktų reikalavimus, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

47. Saugos įgaliotinis yra atsakingas už BPIS naudotojų supažindinimą su BPIS duomenų saugos nuostatais, BPIS saugaus elektroninės informacijos tvarkymo taisyklėmis, Valdymo planu, BPIS naudotojų administravimo taisyklėmis ir kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą.

48. Saugos įgaliotinis planuoja ir ne rečiau kaip kartą per 2 metus organizuoja ir vykdo BPIS vidinių naudotojų mokymus informacijos saugos, kibernetinio saugumo klausimais.

49. Mokymų ir seminarų metu saugos įgaliotinis supažindina administratorių ir BPIS naudotojus su duomenų apsaugos politiką reglamentuojančiais teisės aktais, saugaus darbo su duomenimis principais.

50. Saugos įgaliotinis informuoja BPIS naudotojus el. paštu apie priimtus naujus teisės aktus ir teisės aktų pakeitimus, apie BPIS naudotojams organizuojamus kvalifikacijos tobulinimo ir mokymo renginius, siunčia atmintines priimtiems naujiems BPIS naudotojams.

51. BPIS tvarkymo įstaiga sudaro galimybes BPIS administratoriui ir BPIS naudotojams dalyvauti saugos įgaliotinio organizuojamuose kvalifikacijos tobulinimo ir mokymo renginiuose.

52. Saugos įgaliotinis, per kalendorinius metus įvertinęs BPIS tvarkymo įstaigos rizikos veiksnių galimybes, išnagrinėjęs BPIS nenumatytų situacijų registravimo žurnalo įrašus, du kartus per metus: pirmo pusmečio – iki liepos mėnesio 10 dienos, antro pusmečio – iki kitų metų sausio 10 dienos – rengia BPIS rizikos ataskaitą (toliau – Ataskaita) (3P3 priedas). Ataskaitą tvirtina BPIS tvarkymo įstaigos vadovas.

V SKYRIUS
BPIS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

53. Už vidinių BPIS naudotojų supažindinimą su Saugos nuostatais ir kitais saugos politiką reguliuojančiais teisės aktais bei atsakomybe už šių reikalavimų nesilaikymą yra atsakingas BPIS saugos įgaliotinis.

54. BPIS naudotojai su Saugos nuostatais ir kitais saugos politiką reguliuojančiais teisės aktais ir atsakomybe už šių reikalavimų nesilaikymą supažindinami Saugos nuostatų 44 punkte nustatyta tvarka.

55. Pakartotinai su saugos politiką reguliuojančiais teisės aktais BPIS naudotojai supažindinami tik iš esmės pasikeitus pačiai BPIS arba informacijos saugą reguliuojantiems teisės aktams.

VI SKYRIUS
BAIGIAMOS NUOSTATOS

56. Saugos nuostatai ir saugos politikos įgyvendinimo teisės aktai turi būti peržiūrėti ne rečiau kaip kartą per kalendorinius metus, atlikus rizikos analizę ar informacinių technologijų saugos atitikties vertinimą, įvykus esminiams organizaciniams, technologiniams ar kitiems BPIS pokyčiams.