PATVIRTINTA
Lietuvos aukštųjų mokyklų asociacijos
bendrajam priėmimui organizuoti
prezidento 2011 m. gegužės mėn. 20 d.
įsakymu Nr. 11-03

BENDROJO PRIĖMIMO Į LIETUVOS AUKŠTĄSIAS MOKYKLAS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1.1. Bendrojo priėmimo į Lietuvos aukštąsias mokyklas informacinės sistemos (toliau – BPIS) duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato BPIS saugos politiką.

1.2. Šiuose Saugos nuostatuose vartojamos sąvokos:

BPIS valdytojas – Lietuvos Respublikos švietimo ir mokslo ministro įgaliota institucija – Lietuvos aukštųjų mokyklų asociacija bendrajam priėmimui organizuoti (toliau - LAMA BPO), kuri nustato informacinės sistemos tikslus, užsako, sukuria arba įsigyja ir valdo informacinę sistemą;

Pagrindinis BPIS tvarkytojas – LAMA BPO - juridinis asmuo, pagal informacinės sistemos nuostatus įgaliotas tvarkyti informacinę sistemą ir duomenis, teikti informaciją ir paslaugas;

BPIS tvarkytojas - juridinis asmuo, atliekantis informacinės sistemos nuostatuose numatytas pagrindinio BPIS tvarkytojo funkcijas;

BPIS duomenų teikėjai – Lietuvos Respublikos švietimo ir mokslo institucijos, arba kitos institucijos, pasirašiusios bendradarbiavimo sutartį su pagrindiniu BPIS tvarkytoju ir į šios sistemos duomenų bazes įkeliantys arba šiai sistemai nuolat teikiantys duomenis;

BPIS duomenų gavėjai – registruotos Lietuvos Respublikos švietimo ir mokslo institucijos, nuolat gaunančios BPIS duomenis ir kurioms pagrindinio BPIS tvarkytojo nustatyta tvarka suteikta prieiga prie BPIS, o taip pat elektroninių ryšių paslaugų teikėjai, kuriems duomenys teikiami duomenų teikimo sutartyse nustatytomis sąlygomis;

BPIS naudotojai – registruoti LAMA BPO darbuotojai ir tam tikrų Lietuvos Respublikos švietimo ir mokslo institucijų, kaip BPIS tvarkytojų, darbuotojai, turintys teisę naudotis BPIS ištekliais numatytoms funkcijoms atlikti ir kuriems pagrindinio BPIS tvarkytojo nustatyta tvarka suteikta prieiga prie BPIS;

BPIS kaupiamų duomenų šaltiniai – stojantieji ir stojamųjų egzaminų bei testų vertintojai, Studijų kokybės vertinimo centras (toliau - **SKVC**), Lietuvos mokinių informavimo ir techninės kūrybos centras (toliau - **LMITKC**), Lietuvos mokinių ir studentų sporto centras (toliau - **LMSSC**), Švietimo ir mokslo ministerija (toliau – **ŠMM**), Aukštosios mokyklos, teiksiantys pirminius duomenis BPIS ir kuriems pagrindinio BPIS tvarkytojo nustatyta tvarka suteikta prieiga prie BPIS;

Kitos 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) (toliau – Saugos reikalavimai), Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairėse, patvirtintose Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymu Nr.1V-247 (Žin., 2007, Nr.78- 3160), Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniuose saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2008 m. spalio 27 d. įsakymu Nr.1V-384 (Žin., 2008, Nr.127-4866), LAMA BPO prezidento 2011 m. gegužės 12 d. įsakymu Nr. 11-01 patvirtintuose „Bendrojo priėmimo į Lietuvos aukštąsias mokyklas informacinės sistemos nuostatuose (toliau – BPIS nuostatuose), 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 standartuose LST ISO/IEC 27002:2009 ir LST ISO/IEC 27001:2006 vartojamas sąvokas.

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

1.4. 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.

1.5. BPIS duomenų saugos užtikrinimo prioritetinės kryptys:

1.5.1. BPIS duomenų tvarkymui naudojamos techninės ir programinės įrangos kontrolė;

1.5.2. BPIS duomenų tvarkymo kontrolė;

1.5.3. Naudojimosi BPIS duomenimis kontrolė.

1.6. Saugos nuostatai taikomi:

1.6.1. BPIS valdytojai ir pagrindinei BPIS tvarkytojai – LAMA BPO (Studentų g. 63A, 51369 Kaunas), kuri atlieka šias funkcijas, susijusias su BPIS duomenų sauga:

1.6.1.1. Priima sprendimą dėl BPIS informacinių technologijų atitikties Saugos reikalavimams vertinimo atlikimo;

1.6.1.2. Rengia ir tvirtina teisės aktus, susijusius su BPIS duomenų tvarkymu ir duomenų sauga, ir prižiūri, kaip jų laikomasi;

1.6.1.3. Užtikrina BPIS duomenų bazių techninę priežiūrą;

1.6.1.4. Atsako už BPIS duomenų tvarkymo ir duomenų teikimo/gavimo teisėtumą bei saugą;

1.6.1.5. Skiria BPIS saugos įgaliotinį;

1.6.1.6. Atlieka kitas Saugos nuostatų, Saugos reikalavimų, BPIS nuostatų ir kitų teisės aktų nustatytas funkcijas.

1.6.2. BPIS tvarkytojams ir BPIS duomenų teikėjams (įskaitant juridinius BPIS kaupiamųjų duomenų šaltinius), sudarantiems BPIS organizacinę struktūrą (ir BPIS informacinę infrastruktūrą), kurie:

1.6.2.1. Atsako už BPIS duomenų tvarkymo ir duomenų teikimo/gavimo teisėtumą bei saugą. *BPIS kaupiamųjų duomenų šaltinių duomenų saugai užtikrinti šių įstaigų vadovai skiria jų informacinių sistemų saugos administratorius, kurie už atliekamas saugumo politikos įgyvendinimo ir kontrolės funkcijas atsiskaito tiesiogiai BPIS saugos įgaliotiniui*;

1.6.2.2. Vykdo kitas Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas bei BPIS saugos įgaliotinio nurodymus, susijusius su BPIS naudojimu ir sauga.

1.7. Saugos įgaliotinis organizuoja ir kontroliuoja šių Saugos nuostatų įgyvendinimą ir atlieka kitas funkcijas:

1.7.1. Teikia LAMA BPO prezidentui siūlymus dėl:

1.7.1.1. Saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

1.7.1.2. BPIS saugos reikalavimų atitikties vertinimo atlikimo;

1.7.1.3. BPIS posistemių/funkcijų ir tarnybinių stočių administratorių paskyrimo.

1.7.2. Koordinuoja elektroninės informacijos saugos incidentų tyrimą;

1.7.3. *Teikia BPIS posistemių/funkcijų ir tarnybinių stočių administratoriams privalomus vykdyti nurodymus ir pavedimus*;

1.7.4. Atlieka kitas Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas ir kitus LAMA BPO prezidento nurodymus, susijusius su BPIS sauga.

1.8. BPIS administratoriai:

1.8.1. Tarnybinių stočių administratoriai atsako už BPIS funkcionavimą užtikrinančios techninės ir programinės įrangos darbo užtikrinimą, prieigos prie BPIS infrastruktūros išteklių teisių nustatymą;

1.8.2. Posistemių/funkcijų administratoriai vertina BPIS naudotojų pasirengimą dirbti su BPIS ir suteikia jos naudotojams teises naudotis informacinės sistemos galimybėmis paskirtoms funkcijoms vykdyti.

1.8.3. Pagal kompetenciją rengia pasiūlymus dėl BPIS palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

1.8.4. Registruoja elektroninės informacijos saugos incidentus, informuoja apie juos saugos įgaliotinį ir teikia pasiūlymus dėl minėtų incidentų pašalinimo;

1.9. Teisės aktai, kuriais vadovaujantis tvarkomi BPIS duomenys ir užtikrinama jų sauga:

1.9.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (Žin., 1996, Nr. 63-1479; 2000, Nr. 64-1924; 2003, Nr.15-597);

1.9.2. Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtinti Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71 (Žin., 2008. Nr.135-5298);

1.9.3. Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai, patvirtinti Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891);

1.9.4. BPIS nuostatai;

1.9.5. Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai, patvirtinti Vidaus reikalų Ministerijos *2008 m. spalio 27 d. įsakymu Nr. 1V-384* (Žin., 2008, Nr. 217-4866);

1.9.6. Lietuvos standartai LST ISO/IEC 27002:2009 ir LST ISO/IEC 27001:2006 bei kiti Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, reglamentuojantys saugų informacinės sistemos duomenų tvarkymą;

1.9.7. Kiti teisės aktai, reglamentuojantys BPIS duomenų tvarkymo teisėtumą, BPIS valdytojo ir BPIS duomenų tvarkytojų veiklą bei duomenų saugos valdymą.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

2.1. BPIS tvarkoma elektroninė informacija ir duomenys, kurie yra nurodyti BPIS nuostatuose. Šių duomenų konfidencialumo, vientisumo ir (ar) prieinamumo praradimas gali turėti neigiamą įtaką LAMA BPO veiklai. Informacinėje sistemoje taip pat tvarkomi asmens duomenys. Sutinkamai su 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 (Žin., 2007, Nr. 78-3160; *2008, Nr.127-4866*), BPIS priskiriama trečiajai informacinės sistemos kategorijai.

2.2. BPIS saugos priemonės parenkamos įvertinus galimus rizikos veiksnius BPIS duomenų vientisumui, konfidencialumui ir prieinamumui.

2.3. Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, ne rečiau kaip kartą per 2 metus organizuoja BPIS rizikos įvertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį rizikos įvertinimą. BPIS rizikos veiksnių vertinimui taikoma kokybinė rizikos vertinimo metodika.

2.4. BPIS rizikos įvertinimas išdėstomas rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausieji rizikos veiksniai yra šie:

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

2.4.2. Subjektyvūs tyčiniai (nesankcionuotas naudojimasis BPIS duomenims gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugos pažeidimai, vagystės ir kita);

2.4.3. Nenugalima jėga (force majeure).

2.5. LAMA BPO prezidentas, atsižvelgdamas į BPIS rizikos įvertinimo ataskaitą, prireikus tvirtina saugos įgaliotinio parengtą rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

2.6. Siekiant užtikrinti Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose išdėstytų nuostatų įgyvendinimo kontrolę, saugos įgaliotinis ne rečiau kaip kartą per 2 metus organizuoja BPIS informacinių technologijų saugos reikalavimų atitikties vertinimą, kurio metu:

2.6.1. Įvertinama Saugos nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų atitiktis realiai BPIS duomenų saugos situacijai;

2.6.2. Inventorizuojama BPIS valdytojo kompiuterinė techninė ir programinė įranga;

2.6.3. Tikrinama BPIS tarnybinėse stotyse bei ne mažiau kaip 10 procentų BPIS valdytojo kompiuterizuotose darbo vietose įdiegta programinė įranga ir jos sąranka (konfigūracija);

2.6.4. Peržiūrima BPIS naudotojams suteiktų teisių ir atliekamų funkcijų atitiktis, prireikus BPIS naudotojų teisės praplečiamos arba apribojamos;

2.6.5. Tikrinamos BPIS duomenų gavėjams suteiktos teisės;

2.6.6. Įvertinamas pasirengimas atkurti BPIS veiklos tęstinumą, įvykus BPIS duomenų saugos incidentui.

2.7. Remdamasis atlikto BPIS informacinių technologijų saugos reikalavimų atitikties vertinimo rezultatais, saugos įgaliotinis parengia ir LAMA BPO prezidentui pateikia tvirtinti pastebėtų trūkumų šalinimo planą, kuriame nurodomi atsakingi vykdytojai ir nustatomi numatytų priemonių įgyvendinimo terminai.

2.8. Techninės, programinės ir organizacinės elektroninės informacijos saugos priemonės pasirenkamos taip, kad būtų užtikrintas BPIS veiklos tęstinumas, patiriant kuo mažiau išlaidų ir būtų užtikrintas saugus BPIS naudotojų darbas.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

3.1. BPIS duomenų saugai yra taikomos tam tikros programinės įrangos naudojimo nuostatos:

3.1.1. BPIS tarnybinėse stotyse, BPIS naudotojų kompiuteriuose diegiama tik legali ir saugi programinė įranga (operacinė sistema su naujaisiais pataisymais);

3.1.2. BPIS tarnybinėse stotyse, BPIS naudotojų kompiuteriuose operacinių sistemų ir taikomųjų programų sąranka parenkama tokiu būdu, kad būtų užtikrintas didžiausias saugumo lygis (išjungiami nereikalingi darbui procesai ir reikmenys (angl. services), ribojamas priėjimas prie operacinės sistemos prievadų.)

3.1.3. BPIS tarnybinėse stotyse, BPIS naudotojų kompiuteriuose privalo būti naudojama reguliariai atnaujinama programinė įranga, skirta kovai su kenksminga programine įranga;

3.1.4. BPIS tarnybinėse stotyse neturi veikti programinė įranga, nesusijusi su BPIS duomenų tvarkymu, BPIS naudotojų, BPIS duomenų gavėjų ir pačios įrangos administravimu.

3.1.5. BPIS programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims.

3.2. Kompiuterinis tinklas, prie kurio prijungtos BPIS tarnybinės stotys, nuo viešojo interneto turi būti atskirtas tinklo užkarda (angl. firewall).

3.3. BPIS naudotojų veiksmai su BPIS duomenimis registruojami elektroniniame duomenų keitimo žurnale.

3.4. Tiesioginė prieiga prie BPIS duomenų suteikiama, įgyvendinus BPIS naudotojų autentifikavimo priemones. Tiesioginė prieiga prie BPIS duomenų užtikrinama automatiniu būdu ne mažiau 90 proc. laiko darbo ir poilsio dienomis.

3.5. BPIS duomenys perduodami automatiniu būdu naudojant TCP/IP protokolą realiame laike („ON-line“ režimu) arba asinchroniniu režimu pagal BPIS duomenų teikimo/gavimo sutartis, kuriose nustatytos perduodamų duomenų specifikacijos, perdavimo sąlygos ir tvarka.

3.6. Asmens duomenys, perduodami ne BPIS naudotojams priklausančiomis duomenų perdavimo linijomis, turi būti šifruojami. Duomenų šifravimą privalo užtikrinti BPIS valdytojas.

3.7. BPIS tarnybinių stočių administratoriai atsako už atsarginių BPIS duomenų kopijų darymą ir saugojimą. BPIS duomenų atsarginės kopijos turi būti daromos automatiškai. Turi būti periodiškai atliekama kopijų tinkamumo ir saugojimo kontrolė. Kopijų, iš kurių būtų galima atstatyti BPIS duomenis, darymo ir saugojimo tvarka detaliai aprašoma BPIS saugaus elektroninės informacijos tvarkymo taisyklėse.

IV. REIKALAVIMAI PERSONALUI IR SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

4.1. BPIS saugos įgaliotinis privalo turėti dokumentais patvirtintą informacinių technologijų specialisto kvalifikaciją, išmanyti informacijos saugos užtikrinimo principus, savo darbe vadovautis Saugos reikalavimais bei kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų duomenų tvarkymą, standartais ir kitais dokumentais, sugebėti prižiūrėti, kaip įgyvendinama saugos politika.

4.2. BPIS tarnybinių stočių, posistemių/funkcijų administratoriai privalo išmanyti pagrindinius saugos politikos principus, darbą su duomenų perdavimo tinklais, mokėti užtikrinti jų saugumą, turėti sisteminių programinių priemonių bei duomenų bazių administravimo ir priežiūros patirties, turi būti susipažinę su Saugos nuostatais ir saugos politiką įgyvendinančiais teisės aktais.

4.3. BPIS naudotojai privalo turėti atitinkamą kvalifikaciją (BPIS programinės įrangos naudotojų mokymai, pradinis saugaus darbo su duomenimis mokymas ar pan.) ir patirties (dirbant su WINDOWS operacinėmis sistemomis, taikomosiomis programomis ir pan.).

4.4. Tvarkyti BPIS duomenis gali tik tie BPIS pagrindinio duomenų tvarkytojo darbuotojai ir tik tie stojamųjų egzaminų ir testų vertintojai, kurie susipažinę su Saugos nuostatais ir kitais saugos politiką įgyvendinančiais teisės aktais ir raštiškai sutikę laikytis šių teisės aktų reikalavimų.

4.5. Tvarkyti BPIS duomenis gali tik tie BPIS naudotojai, kurie susipažinę su Saugos nuostatais ir kitais saugos politiką įgyvendinančiais teisės aktais ir patvirtino savo sutikimą laikytis šių teisės aktų reikalavimų.

4.6. BPIS naudotojų supažindinimą su Saugos nuostatais ir kitais saugos politiką įgyvendinančiais teisės aktais ir atsakomybe už šių reikalavimų nesilaikymą organizuoja saugos įgaliotinis. Saugos įgaliotinis informuoja BPIS naudotojus apie Saugos nuostatų pakeitimus ar kitų saugos politiką įgyvendinančių teisės aktų pripažinimą netekusiais galios, keitimą ar priėmimą. BPIS nuostatai ir Saugos nuostatai skelbiami LAMA BPO tinklalapyje.

4.7. BPIS naudotojams turi būti nuolat rengiami duomenų saugos mokymai, įvairiais būdais primenama apie saugos problematiką (pvz., priminimai elektroniniu būdu, teminių seminarų rengimas ir pan.). *Už saugumo problemų priminimą, mokymų organizavimą atsako BPIS saugos įgaliotinis.*

4.8. BPIS naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veiklos požymių, neveikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti atitinkamam administratoriui, o jo nesant - BPIS saugos įgaliotiniui.

V. BAIGIAMOSIOS NUOSTATOS

5.1. BPIS saugos įgaliotinis, BPIS tarnybinių sočių bei funkcijų/posistemių administratoriai, BPIS naudotojai, pažeidę Saugos nuostatų ar kitų saugos politikos įgyvendinimą reglamentuojančių dokumentų reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

5.2. Saugos nuostatai turi būti peržiūrimi ne rečiau kaip kartą per 3 (tris) metus.

5.3. BPIS valdytojas Saugos nuostatus gali keisti arba pripažinti netekusiais galios savo arba Saugos įgaliotinio iniciatyva.

_____

SUDERINTA
Vidaus reikalų ministerijos
2011 m. vasario 22 d. raštu Nr. ID-1352(6)

SUDERINTA
ŠMM švietimo Informacinių Technologijų Centro
2011 m. gegužės 19 d. raštu Nr. 90-(1.6)-D3-253