

PATVIRTINTA
Lietuvos nacionalinės M. Mažvydo
bibliotekos generalinio direktoriaus
2009 m. rugpjūčio 17 d.
įsakymu Nr.B-133

LIETUVOS INTEGRALIOS BIBLIOTEKŲ INFORMACIJOS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Lietuvos integralios bibliotekų informacijos sistemos (toliau – LIBIS) duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja LIBIS saugos politiką.

2. Šiuose Saugos nuostatuose vartojamos sąvokos:

LIBIS tvarkytojas ir valdytojas – Lietuvos nacionalinė Martyno Mažvydo biblioteka (toliau – Nacionalinė biblioteka).

LIBIS duomenų tvarkytojai – specialiosios, akademinės, apskričių, miestų bei rajonų viešosios bibliotekos, muziejai, pildantys savo elektroninių katalogų duomenis ir pagal sutartis su Nacionaline biblioteka teikiantys duomenis į LIBIS.

LIBIS naudotojai – LIBIS tvarkytojas ir valdytojas bei LIBIS duomenų tvarkytojai, kurie turi teisę naudotis LIBIS ištekliais numatytoms funkcijoms atlikti. Jeigu toliau tekste LIBIS naudotojams keliami konkretūs reikalavimai dėl LIBIS duomenų saugos veiksmų, tai LIBIS naudotojas suprantamas kaip konkretus fizinis asmuo, kuriam suteikta teisė naudotis LIBIS ištekliais jo funkcijoms vykdyti.

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), Nacionalinės bibliotekos generalinio direktoriaus patvirtintuose Lietuvos integralios bibliotekų informacijos sistemos nuostatuose (toliau – LIBIS 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 17799:2006 ir LST ISO/IEC 27001:2006 vartojamas sąvokas.

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

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

5. LIBIS duomenų saugos užtikrinimo prioritetinės kryptys:

5.1. LIBIS duomenų tvarkymui naudojamos techninės ir programinės įrangos kontrolė;

5.2. LIBIS duomenų tvarkymo kontrolė;

5.3. Naudojimosi LIBIS duomenimis kontrolė.

6. Saugos nuostatai taikomi:

6.1. LIBIS valdytojai ir tvarkytojai – Nacionalinei bibliotekai (Gedimino pr. 51, LT – 01504, Vilnius), kuri atlieka šias funkcijas, susijusias su LIBIS duomenų sauga:

6.1.1. Priima sprendimą dėl LIBIS informacinių technologijų atitikties Saugos reikalavimams vertinimo atlikimo;

- 6.1.2. Rengia ir tvirtina teisės aktus, susijusius su LIBIS duomenų tvarkymu ir duomenų sauga, ir prižiūri, kaip jų laikomasi;
- 6.1.3. Užtikrina LIBIS duomenų bazių techninę priežiūrą;
- 6.1.4. Atsako už LIBIS duomenų tvarkymo ir duomenų teikimo/gavimo teisėtumą bei saugą.
- 6.1.5. Skiria LIBIS saugos įgaliotinį.
- 6.1.6. Atlieka kitas Saugos nuostatų, Saugos reikalavimų, LIBIS nuostatų ir kitų teisės aktų nustatytas funkcijas.
- 6.2. LIBIS duomenų tvarkytojams, sudarantiems LIBIS informacinę infrastruktūrą, kurie:
 - 6.2.1. Atsako už LIBIS duomenų tvarkymo ir duomenų teikimo/gavimo teisėtumą bei saugą.
 - 6.2.2. *LIBIS duomenų tvarkytojų duomenų saugai užtikrinti šių įstaigų vadovai skiria jų informacinių sistemų saugos administratorius, kurie už atliekamas saugumo politikos įgyvendinimo ir kontrolės funkcijas atsiskaito tiesiogiai LIBIS saugos įgaliotiniui.*
 - 6.2.3. Vykdo kitas Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas bei LIBIS saugos įgaliotinio nurodymus, susijusius su LIBIS naudojimu ir sauga.
- 7. Saugos įgaliotinis organizuoja ir kontroliuoja šių Saugos nuostatų įgyvendinimą ir atlieka kitas funkcijas:
 - 7.1. Teikia Nacionalinės bibliotekos generaliniam direktoriui siūlymus dėl:
 - 7.1.1. Saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;
 - 7.1.2. LIBIS saugos reikalavimų atitikties vertinimo atlikimo;
 - 7.1.3. LIBIS posistemų/funkcijų ir tarnybinių stočių administratorių paskyrimo.
 - 7.2. Koordinuoja elektroninės informacijos saugos incidentų tyrimą;
 - 7.3. *Teikia LIBIS posistemų/funkcijų ir tarnybinių stočių administratoriams privalomus vykdyti nurodymus ir pavedimus;*
 - 7.4. Atlieka kitas Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas ir kitus Nacionalinės bibliotekos generalinio direktoriaus nurodymus, susijusius su LIBIS sauga.
- 8. LIBIS administratoriai:
 - 8.1. Tarnybinių stočių administratoriai atsako už LIBIS funkcionavimą užtikrinančios techninės ir programinės įrangos darbo užtikrinimą, prieigos prie LIBIS infrastruktūros išteklių teisių nustatymą;
 - 8.2. Posistemų/funkcijų administratoriai vertina LIBIS naudotojų pasirengimą dirbti su LIBIS ir suteikia jos naudotojams teises naudotis informacinės sistemos galimybėmis paskirtoms funkcijoms vykdyti.
 - 8.3. Pagal kompetenciją rengia pasiūlymus dėl LIBIS palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;
 - 8.4. Registruoja elektroninės informacijos saugos incidentus, informuoja apie juos saugos įgaliotinį ir teikia pasiūlymus dėl minėtų incidentų pašalinimo;
- 9. Teisės aktai, kuriais vadovaujantis tvarkomi LIBIS duomenys ir užtikrinama jų sauga:
 - 9.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (Žin., 1996, Nr. 63-1479; 2000, Nr. 64-1924; 2003, Nr.15-597);
 - 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);

- 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).
- 9.4. LIBIS nuostatai;
- 9.5. Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai, patvirtinti Vidaus reikalų Ministerijos 2008 m. spalio 27 d. įsakymu Nr. IV-384 (Žin., 2008, Nr. 217-4866);
- 9.6. Lietuvos standartai LST ISO/IEC 17799:2006 ir LST ISO/IEC 27001:2006 bei kiti Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, reglamentuojantys saugų informacinės sistemos duomenų tvarkymą;
- 9.7. Kiti teisės aktai, reglamentuojantys LIBIS duomenų tvarkymo teisėtumą, LIBIS valdytojo ir LIBIS duomenų tvarkytojų veiklą bei duomenų saugos valdymą.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

10. LIBIS tvarkoma elektroninė informacija, kuri yra nurodyta LIBIS nuostatuose. Šių duomenų konfidencialumo, vientisumo ir (ar) prieinamumo praradimas gali turėti neigiamą įtaką Nacionalinės bibliotekos 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), LIBIS priskiriama trečiajai informacinės sistemos kategorijai.

11. LIBIS saugos priemonės parenkamos įvertinus galimus rizikos veiksnius LIBIS duomenų vientisumui, konfidencialumui ir prieinamumui.

12. 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 LIBIS rizikos įvertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį rizikos įvertinimą. LIBIS rizikos veiksnių vertinimui taikoma kokybinė rizikos vertinimo metodika.

13. LIBIS rizikos įvertinimas išdėstomas rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausieji 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 kita);
- 13.2. Subjektyvūs tyčiniai (nesankcionuotas naudojimas LIBIS duomenims gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugos pažeidimai, vagystės ir kita);
- 13.3. Nenugalima jėga (force majeure).

14. Nacionalinės bibliotekos generalinis direktorius, atsižvelgdamas į LIBIS 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.

15. 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 LIBIS informacinių technologijų saugos reikalavimų atitikties vertinimą, kurio metu:

- 15.1. Įvertinama Saugos nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų atitiktis realiai LIBIS duomenų saugos situacijai;
- 15.2. Inventorizuojama LIBIS valdytojo kompiuterinė techninė ir programinė įranga;
- 15.3. Tikrinama LIBIS tarnybinėse stotyse bei ne mažiau kaip 10 procentų LIBIS valdytojo kompiuterizuotose darbo vietose įdiegta programinė įranga ir jos sąranka (konfigūracija);
- 15.4. Peržiūrima LIBIS naudotojams suteiktų teisių ir atliekamų funkcijų atitiktis, prireikus LIBIS naudotojų teisės praplečiamos arba apribojamos;
- 15.5. Tikrinamos LIBIS duomenų gavėjams suteiktos teisės;
- 15.6. Įvertinamas pasirengimas atkurti LIBIS veiklos tęstinumą, įvykus LIBIS duomenų saugos incidentui.

16. Remdamasis atlikto LIBIS informacinių technologijų saugos reikalavimų atitikties vertinimo rezultatais, saugos įgaliotinis parengia ir Nacionalinės bibliotekos generaliniam direktoriui pateikia tvirtinti pastebėtų trūkumų šalinimo planą, kuriame nurodomi atsakingi vykdytojai ir nustatomi numatytų priemonių įgyvendinimo terminai.

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

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

18. LIBIS duomenų saugai yra taikomos tam tikros programinės įrangos naudojimo nuostatos:

- 18.1. LIBIS tarnybinėse stotyse, LIBIS naudotojų kompiuteriuose diegiama tik legali ir saugi programinė įranga (operacinė sistema su naujaisiais pataisymais);
- 18.2. LIBIS tarnybinėse stotyse, LIBIS 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 priedavų.)
- 18.3. LIBIS tarnybinėse stotyse, LIBIS naudotojų kompiuteriuose privalo būti naudojama reguliariai atnaujinama programinė įranga, skirta kovai su kenksminga programine įranga.
- 18.4. LIBIS tarnybinėse stotyse neturi veikti programinė įranga, nesusijusi su LIBIS duomenų tvarkymu, LIBIS naudotojų, LIBIS duomenų gavėjų ir pačios įrangos administravimu.
- 18.5. LIBIS programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims.

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

20. LIBIS naudotojų veiksmai su LIBIS duomenimis registruojami elektroniniame duomenų keitimo žurnale.

21. Tiesioginė prieiga prie LIBIS duomenų suteikiama, įgyvendinus LIBIS naudotojų autentifikavimo priemones. Tiesioginė prieiga prie LIBIS duomenų užtikrinama automatiškai būdu ne mažiau 90 proc. laiko darbo ir poilsio dienomis.

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

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

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

IV. REIKALAVIMAI PERSONALUI IR SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

25. LIBIS 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.

26. LIBIS 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

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

28. Tvarkyti LIBIS duomenis gali tik LIBIS naudotojai, kurie susipažinę su Saugos nuostatais ir kitais saugos politiką įgyvendinančiais teisės aktais ir raštiškai sutikę laikytis šių teisės aktų reikalavimų.

29. LIBIS naudotojų supažindinimą su Saugos nuostatais ir kitais saugos politiką įgyvendinančiais teisės aktais ir atsakomybę už šių reikalavimų nesilaikymą organizuoja saugos įgaliotinis. Saugos įgaliotinis informuoja LIBIS naudotojus apie Saugos nuostatų pakeitimus ar kitų saugos politiką įgyvendinančių teisės aktų pripažinimą netekusiais galios, keitimą ar priėmimą. LIBIS nuostatai ir Saugos nuostatai skelbiami Nacionalinės bibliotekos tinklalapyje.

30. LIBIS 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 LIBIS saugos įgaliotinis.*

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

V. BAIGIAMOSIOS NUOSTATOS

32. LIBIS saugos įgaliotinis, LIBIS tarnybinių stočių bei funkcijų/posistemių administratoriai, LIBIS naudotojai, pažeidę Saugos nuostatų ar kitų saugos politiką įgyvendinančių teisės aktų reikalavimus, atsako įstatymų nustatyta tvarka.

SUDERINTA

Vidaus reikalų ministerijos

2009 m. liepos 27 d. raštu Nr.1D-5672 - (13)