

PATVIRTINTA
Lietuvos Respublikos
švietimo ir mokslo ministro
2015 m. liepos 2 d. įsakymu Nr. V-710

LIETUVOS AKADEMINĖS ELEKTRONINĖS BIBLIOTEKOS INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Lietuvos akademinės elektroninės bibliotekos informacinės sistemos (toliau – eLABa) naudotojų administravimo taisyklės (toliau – Naudotojų administravimo taisyklės) reglamentuoja sistemos naudotojų įgaliojimus, teises, pareigas, jų supažindinimo su saugos dokumentais tvarką ir saugaus sistemoje tvarkomų duomenų teikimo sistemos naudotojams kontrolės tvarką.

2. Naudotojų administravimo taisyklės taikomos visiems eLABa naudotojams ir eLABa administratoriams.

3. eLABa naudotojai ir eLABa administratoriai turi turėti tik tiek priėjimo prie duomenų teisių, kiek tai būtina jų tiesioginei veiklai vykdyti.

4. Naudotojų administravimo taisyklės parengtos, vadovaujantis 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“, Techninių 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“, Lietuvos akademinės elektroninės bibliotekos informacinės sistemos nuostatais ir Lietuvos akademinės elektroninės bibliotekos informacinės sistemos duomenų saugos nuostatais, patvirtintais Lietuvos Respublikos švietimo ir mokslo ministro 2014 m. rugsėjo 22 d. įsakymu Nr. V-838 „Dėl švietimo ir mokslo ministro 2006 m. liepos 14 d. įsakymo Nr. ISAK-1506 „Dėl Lietuvos mokslo ir studijų elektroninių dokumentų informacinės sistemos (eLABa) įsteigimo“ pakeitimo“, ir kitais teisės aktais.

5. Naudotojų administravimo taisyklėse vartojamos sąvokos ir sutrumpinimai:

5.1. **Metaduomenys** – duomenys apie duomenis. Struktūrizuotas eLABa saugomo el. objekto savybių aprašymas naudojant tam tikrus bibliografinio aprašo formatus (*MARC21*, *Dublin Core*; *TEI Header 5* ir kt.).

5.2. **ETD** – elektroninių tezių ir disertacijų duomenų bazė, skirta kaupti Lietuvos mokslo ir studijų institucijų tvirtinamus studijų baigiamuosius darbus, daktaro disertacijas ir jų santraukas ir tvarkyti jų metaduomenis.

5.3. **PDB** – mokslo ir studijų institucijų publikacijų duomenų bazė, skirta kaupti Lietuvos mokslo ir studijų institucijų dėstytojų, mokslo darbuotojų ir studentų paskelbtas publikacijas ir tvarkyti jų metaduomenis.

5.4. **EPAS** – dokumentų sutapties nustatymo sistema – eLABa posistemė, skirta dokumentų panašumo nustatymui ir plagiato kontrolės funkcijos vykdymui.

5.5. Kitos eLABa Naudotojų administravimo taisyklėse vartojamos sąvokos suprantamos taip, kaip apibrėžtos eLABa saugaus elektroninės informacijos tvarkymo taisyklėse ir 4 punkte nurodytuose norminiuose dokumentuose.

II SKYRIUS

eLABa NAUDOTOJŲ IR ADMINISTRATORIŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

6. eLABa naudotojų įgaliojimai, teisės ir pareigos tvarkant elektroninę informaciją:

6.1. eLABa naudotojai gali naudotis tik tomis eLABa funkcijomis ir eLABa tvarkomais duomenimis, prie kurių prieigą jiems suteikė naudotojų teisių administratorius;

6.2. eLABa naudotojai turi teisę rinkti, tvarkyti, perduoti, įkelti, saugoti, naikinti ar kitaip naudoti elektroninę informaciją, tik atlikdami savo tiesiogines funkcijas;

6.3. baigę darbą, naudotojai turi atsijungti nuo eLABa ir uždaryti programinę įrangą;

6.4. eLABa naudotojai privalo:

6.4.1. užtikrinti jų eLABa tvarkomų duomenų konfidencialumą bei vientisumą;

6.4.2. savo veiksmais netrikdyti eLABa duomenų prieinamumo;

6.4.3. jungtis prie eLABa, įvedant tik asmeniškai suteiktus prisijungimo vardus ir slaptažodžius;

6.4.4. nesijungti prie eLABa, naudojantis kitam naudotojui suteiktais prisijungimo vardais ir slaptažodžiais;

6.4.5. neatskleisti, nelaikyti matomoje vietoje suteiktų prisijungimo vardų ir slaptažodžių;

6.4.6. prisiimti atsakomybę už tvarkomų duomenų rinkimą, įvedimą, naikinimą ir kt.;

6.4.7. prisiimti atsakomybę už tinkamą elektroninės informacijos tvarkymo programinių priemonių naudojimą ir techninių priemonių saugojimą;

6.4.8. nedelsiant pranešti tvarkančios institucijos eLABa naudotojų teisių administratoriui apie informacinės sistemos sutrikimus, neįprastą jų veikimą, esamus arba galimus elektroninės informacijos saugumo reikalavimų pažeidimus, kitų eLABa naudotojų nederamus veiksmus;

6.5. eLABa naudotojai skirstomi į autorius, darbo vadovus, institucijų atsakingus asmenis, bibliotekininkus, institucijų padalinių registratorius, institucijų registratorius.

6.5.1. Autoriams suteikiama teisė:

6.5.1.1. įkelti savo ETD ir(ar) PDB dokumentus, kurti ir redaguoti jų metaduomenis;

6.5.1.2. peržiūrėti savo ETD ir(ar) PDB dokumentus bei jų metaduomenis, kurie į sistemą buvo įkelti kitų eLABa naudotojų;

6.5.1.3. formuoti savo duomenų ataskaitas.

6.5.2. Darbo vadovams suteikiama teisė:

6.5.2.1. peržiūrėti, redaguoti, tvirtinti ETD dokumentus;

6.5.2.2. peržiūrėti, redaguoti jiems priskirtų ETD dokumentų tikrinimo EPAS rezultatus.

6.5.3. Institucijų atsakingiems asmenims suteikiama teisė:

6.5.3.1. peržiūrėti jiems priskirtus ETD dokumentus bei dokumentų tikrinimo EPAS rezultatus.

6.5.4. Bibliotekininkams suteikiama teisė:

6.5.4.1. peržiūrėti, įvesti, redaguoti ir tvirtinti visų savo institucijos dokumentų metaduomenis;

6.5.4.2. peržiūrėti visus savo institucijos autorių dokumentus ir jų metaduomenis, kurie buvo pateikti į sistemą kitų institucijų;

6.5.4.3. įvesti, redaguoti ir tvirtinti specifinius savo institucijai metaduomenis dokumentams, pateiktiems į sistemą kitų institucijų;

6.5.4.4. formuoti savo institucijos ataskaitas.

6.5.5. Institucijų padalinių registratoriams suteikiama teisė:

6.5.5.1. įkelti savo institucijos padalinio autorių dokumentus, įvesti ir redaguoti jų metaduomenis;

6.5.5.2. formuoti savo institucijos padalinio ataskaitas.

6.5.6. Institucijų registratoriams suteikiama teisė:

6.5.6.1. peržiūrėti visus savo institucijos autorių dokumentus ir jų metaduomenis;

6.5.6.2. įvesti, redaguoti ir tvirtinti specifinius savo institucijai metaduomenis savo institucijos autorių dokumentams;

6.5.6.3. formuoti savo institucijos ataskaitas.

7. eLABa pagrindinio administratoriaus įgaliojimai, teisės ir pareigos tvarkant elektroninę informaciją:

7.1. teikia privalomus vykdyti nurodymus eLABa sisteminiams, taikomosios programinės įrangos ir savo institucijos naudotojų teisių administratoriams;

7.2. eLABa administravimo klausimais bendradarbiauja su kitų eLABa tvarkytojų įgaliojais asmenimis;

7.3. informuoja eLABa saugos įgaliojimą apie saugos dokumentų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones;

7.4. vykdo eLABa saugos įgaliojimo nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu;

7.5. vykdo kitas tiesiogiai su eLABa administravimu susijusias funkcijas.

8. eLABa sisteminių administratorių įgaliojimai, teisės ir pareigos tvarkant elektroninę informaciją:

8.1. užtikrina eLABa sisteminės programinės įrangos ir duomenų bazių valdymo programinės įrangos veikimą;

8.2. prižiūri eLABa sisteminę programinę įrangą ir duomenų bazių valdymo programinę įrangą;

8.3. daro atsarginių eLABa duomenų kopijas;

8.4. atlieka visišką ar dalinius duomenų atkūrimo bandymus iš atsarginių eLABa saugomų duomenų kopijų;

8.5. užtikrina eLABa sisteminės programinės įrangos saugą;

8.6. nustato eLABa pažeidžiamas vietas ir informuoja apie jas eLABa saugos įgaliojimą;

8.7. vykdo eLABa saugos įgaliojimo nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu.

9. eLABa taikomosios programinės įrangos administratorių įgaliojimai, teisės ir pareigos tvarkant elektroninę informaciją:

9.1. užtikrina eLABa taikomosios programinės įrangos veikimą;

9.2. vykdo eLABa taikomosios programinės įrangos priežiūrą;

9.3. tvarko visų eLABa naudotojų identifikavimo ir suteiktų teisių duomenis;

9.4. prireikus stebi eLABa naudotojų su eLABa tvarkomais duomenimis atliktus veiksmus;

9.5. atlieka su eLABa administravimu susijusias užklausas ir gauna ataskaitas;

9.6. prireikus tvarko ir administruoja visų institucijų paskyrų duomenis;

9.7. vykdo eLABa saugos įgaliojimo nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu;

9.8. informuoja eLABa saugos įgaliojimą apie saugos dokumentų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones;

9.9. vykdo pareigas ir reikalavimus, nurodytus kituose eLABa saugos dokumentuose;

9.10. vykdo kitas tiesiogiai su eLABa administravimu susijusias funkcijas.

10. eLABa naudotojų teisių administratorių įgaliojimai, teisės ir pareigos, tvarkant elektroninę informaciją:

10.1. tvarko ir administruoja savo institucijos eLABa klasifikatorius;

10.2. vykdo savo institucijos eLABa naudotojų ir jų prieigos teisių administravimą;

10.3. vertina savo institucijos eLABa naudotojų pasirengimą dirbti su eLABa;

10.4. atlieka savo institucijos eLABa naudotojams suteiktų teisių ir priskirtų funkcijų atitikties vertinimą;

10.5. konsultuoja savo institucijos eLABa naudotojus dėl eLABa veikimo ir kitais su eLABa susijusiais klausimais;

10.6. reikalauja, kad institucijos eLABa naudotojai vykdytų duomenų saugos ir naudotojų administravimo taisyklių reikalavimus;

10.7. informuoja eLABa saugos įgaliotinį apie saugos dokumentų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones;

10.8. vykdo pareigas ir reikalavimus, nurodytus kituose eLABa saugos dokumentuose;

10.9. vykdo eLABa saugos įgaliotinio ir pagrindinio administratoriaus nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu;

10.10. pagrindinio administratoriaus nurodymu vykdo kitas tiesiogiai su eLABa naudotojų teisių administravimu susijusias funkcijas.

11. eLABa lokalaus tinklo ir darbo vietų administratorių įgaliojimai, teisės ir pareigos tvarkant elektroninę informaciją:

11.1. užtikrina savo institucijos lokalių tinklų veikimą;

11.2. prižiūri savo institucijos lokalius tinklus;

11.3. užtikrina eLABa naudotojų kompiuterinių darbo vietų saugą ir sklandų veikimą savo institucijoje;

11.4. prižiūri eLABa naudotojų kompiuterines darbo vietas savo institucijoje;

11.5. diegia, atnauja antivirusines programas savo institucijos eLABa naudotojų darbo vietose;

11.6. vykdo pareigas ir reikalavimus, nurodytus kituose eLABa saugos dokumentuose;

11.7. vykdo kitas tiesiogiai su eLABa naudotojų lokalaus tinklo ir darbo vietų administravimu susijusias funkcijas.

III SKYRIUS

SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO eLABa NAUDOTOJAMS KONTROLĖS TVARKA

12. eLABa naudotojų registravimo ir išregistravimo tvarka:

12.1. eLABa naudotojai įregistruojami, įvedant jų duomenis į sistemą rankiniu būdu arba importuojant iš nustatyto formato rinkmenų, suformuojamų atitinkamo eLABa tvarkytojo informacinės sistemos;

12.2. už eLABa naudotojų duomenų įvedimą ir jų atnaujinimą laiku yra atsakingi naudotojų teisių administratoriai;

12.3. eLABa tvarkytojas, paskyręs eLABa naudotojų teisių administratorių, kreipiasi į pagrindinį eLABa tvarkytoją raštu su prašymu suteikti prieigą prie jam reikalingų funkcijų eLABa, kartu pateikdamas paskirto asmens sutikimą tvarkyti asmens duomenis ir pasižadėjimą laikytis eLABa saugos dokumentų reikalavimų;

13. Priemonės eLABa naudotojų tapatybei nustatyti:

13.1. eLABa naudotojui jungiantis į sistemą, jo tapatybė nustatoma pagal unikalų eLABa naudotojo identifikatorių, patvirtinamą asmeniniu slaptažodžiu.

14. eLABa naudotojų slaptažodžio sudarymo, galiojimo trukmės ir keitimo reikalavimai:

14.1. eLABa naudotojų slaptažodžiai turi būti sudaryti iš 8–20 ženklų ir turėti bent 1 skaičių ir 1 raidę. Negalima naudoti lengvai nuspėjamų (pvz., vartotojo vardo, gimimo datos ir t. t.) slaptažodžių. Slaptažodis turi būti keičiamas ne rečiau kaip kas 3 mėnesius;

14.2. draudžiama slaptažodžius atskleisti tretiesiems asmenims;

14.3. leistinas mėginimų įvesti teisingą slaptažodį skaičius yra 5 kartai; slaptažodį neteisingai įvedus didžiausią leistiną skaičių, informacinė sistema užsirakina ir neleidžia informacinės sistemos naudotojui identifikuotis mažiausiai 15 minučių;

14.4. slaptažodžiai negali būti saugomi ar perduodami atviru tekstu ar užšifruojami nepatikimais algoritmais; saugos įgaliotinio sprendimu tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jei:

14.4.1. eLABa naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio;

14.4.2. nėra techninių galimybių eLABa naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu;

14.5. eLABa sisteminių ir taikomosios programinės įrangos administratorių slaptažodžiams yra keliami šie reikalavimai:

14.5.1. eLABa sisteminių ir taikomosios programinės įrangos administratorių slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius;

14.5.2. eLABa sisteminių ir taikomosios programinės įrangos administratorių slaptažodis turi būti iš ne trumpesnės kaip 12 simbolių kombinacijos, sudarytos iš didžiųjų, mažųjų raidžių, skaitmenų ir specialiųjų simbolių;

14.5.3. keičiant slaptažodį, eLABa neturi leisti sudaryti slaptažodžio iš buvusių 3 paskutinių slaptažodžių.

15. Sąlygos ir atvejai, kai panaikinama eLABa naudotojų teisė dirbti su konkrečia elektronine informacija:

15.1. eLABa tvarkytojo darbuotojui prieiga prie konkrečios elektroninės informacijos turi būti sustabdoma, kai eLABa tvarkytojo darbuotojas nušalinamas nuo darbo (pareigų); pasibaigus tarnybos (darbo) santykiams. eLABa tvarkytojo darbuotojo teisė naudotis eLABa turi būti panaikinta nedelsiant;

15.2. eLABa taikomosios programinės įrangos administratorius, iš pagrindinio eLABa tvarkytojo gavęs rašytinį prašymą apriboti eLABa naudotojo prieigos teises, nedelsiant sustabdo nurodyto eLABa naudotojo prieigą prie eLABa;

15.3. eLABa naudotojams prieigos prie eLABa teisės nutraukiamos automatiškai, sistemai nustačius naudotojo darbo ar studijų konkrečioje institucijoje pabaigos datą (jei eLABa naudotojas nustoja dirbti ar studijuoti konkrečioje institucijoje, jis negali jungtis į eLABa kaip tos institucijos naudotojas);

15.4. institucijos arba sistemos administratorius, gavęs įgalioto institucijos darbuotojo nurodymą, gali sustabdyti eLABa naudotojo prieigą prie sistemos rankiniu būdu, nepriklausomai nuo eLABa naudotojo darbo ar studijų konkrečioje institucijoje galiojimo;

15.5. esant būtinybei, jei kyla grėsmė eLABa duomenų saugumui, institucijos arba sistemos administratorius turi sustabdyti eLABa naudotojo prieigą savarankiškai, informuodamas apie tai įgaliotą institucijos darbuotoją;

15.6. eLABa administratoriui teisė dirbti su konkrečia elektronine informacija yra ribojama, sustabdant visas eLABa administratoriui suteiktas prieigos prie eLABa teises, kai eLABa administratorius nesijungė prie sistemos daugiau nei tris mėnesius, vyksta eLABa administratoriaus veiklos tyrimas, eLABa administratorius neteikia informacijos apie saugą užtikrinančių sistemos komponentų būklę ar atsisako vykdyti saugos įgaliotinio nurodymus ir pavedimus;

15.7. kai eLABa vidinis naudotojas ar administratorius perkeliamas į kitas pareigas, ne vėliau kaip per 5 darbo dienas jam suteiktos teisės pakeičiamos, atsižvelgiant į jo pareigybės aprašyme nurodytas funkcijas.

16. Leistini nuotolinio prisijungimo būdai:

16.1. nuotoliniam prisijungimui prie informacinės sistemos eLABa išoriniams naudotojams papildomi reikalavimai nekeliami;

16.2. nuotolinis sisteminių ir taikomosios programinės įrangos administratorių prisijungimas prie eLABa tarnybinių stočių galimas, tik naudojantis VPN tuneliu;

16.3. eLABa viso teksto dokumentų pateikimas, atsižvelgiant į nustatytas prieigos sąlygas, gali būti papildomai kontroliuojamas pagal besijungiančio kompiuterio IP adresą.
