LIETUVOS RESPUBLIKOS ŠVIETIMO, MOKSLO IR SPORTO MINISTRAS

ĮSAKYMAS
DĖL LIETUVOS RESPUBLIKOS ŠVIETIMO IR MOKSLO MINISTRO 2006 M. LIEPOS 14 D. ĮSAKYMO NR. ISAK-1506 „DĖL LIETUVOS AKADEMINĖS ELEKTRONINĖS BIBLIOTEKOS INFORMACINĖS SISTEMOS NUOSTATŲ IR LIETUVOS AKADEMINĖS ELEKTRONINĖS BIBLIOTEKOS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO

2019 m. spalio 14 d. V-1149
Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 43 straipsnio 2 dalimi, Bendrųjų elektroninės informacijos saugos reikalavimų 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“, 8 punktu,

p a k e i č i u Lietuvos akademinės elektroninės bibliotekos informacinės sistemos duomenų saugos nuostatus, patvirtintus Lietuvos Respublikos švietimo ir mokslo ministro 2006 m. liepos 14 d. įsakymu Nr. ISAK-1506 „Dėl Lietuvos akademinės elektroninės bibliotekos informacinės sistemos nuostatų ir Lietuvos akademinės elektroninės bibliotekos informacinės sistemos duomenų saugos nuostatų patvirtinimo“, ir išdėstau juos nauja redakcija (pridedama).

Švietimo, mokslo ir sporto ministras Algirdas Monkevičius

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2019 m. liepos 1 d. raštu Nr. (4.2 E) 6K-424

PATVIRTINTA
Lietuvos Respublikos švietimo ir mokslo ministro 2006 m. liepos 14 d. įsakymu Nr. ISAK-1506
(Lietuvos Respublikos švietimo, mokslo ir sporto ministro 2019 m. spalio 14 d. įsakymo Nr. V-1149 redakcija)

LIETUVOS AKADEMINĖS ELEKTRONINĖS BIBLIOTEKOS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos akademinės elektroninės bibliotekos informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja elektroninės informacijos ir kibernetinio saugumo užtikrinimo ir valdymo principus ir politiką (toliau – Saugos politika), kuria vadovaujantis turi būti įgyvendinama Lietuvos akademinės elektroninės bibliotekos informacinės sistemos (toliau – eLABa), eLABa duomenų saugos procese dalyvaujančių subjektų funkcijos, nustato organizacinius ir techninius duomenų saugos reikalavimus, eLABa naudotojų supažindinimo su eLABa saugos dokumentais principus.

2. Saugos nuostatuose vartojamos sąvokos:

2.1. **eLABa duomenų valdytojai** – eLABa naudojančios institucijos, kiekviena atskirai valdančios savo institucijos ir tvarkančios kitų duomenų valdytojų ir duomenų subjektų eLABa duomenis bei kartu sistemai, bei atskirai savo institucijoje, nustatančios asmens duomenų tvarkymo eLABa tikslus ir priemones;

2.2. **eLABa lokalaus tinklo ir / ar darbo vietų administratorius** – eLABa tvarkytojo ar duomenų valdytojo darbuotojas, kuriam paskirta pareiga vykdyti lokalaus tinklo, naudotojų darbo vietų priežiūrą;

2.3. **eLABa naudotojas** – kitas nei Saugos nuostatų 2.1–2.2, 2.4–2.8 papunkčiuose įvardintas juridinis arba fizinis asmuo, nesantis valdytojo patvirtintu eLABa tvarkytoju, sutartiniais pagrindais naudojantis ir (ar) tvarkantis tik savo asmens eLABa elektroninę informaciją;

2.4. **eLABa naudotojų teisių administratorius** – pagrindinio eLABa tvarkytojo arba eLABa tvarkytojo darbuotojas, kuriam atitinkamas tvarkytojas priskyrė pareigą ir teisę suteikti eLABa naudotojams teises, atitinkamoms eLABa funkcijoms atlikti;

2.5. **eLABa sisteminis administratorius** – pagrindinio eLABa tvarkytojo paskirtas darbuotojas, vykdantis eLABa operacinių sistemų, duomenų bazių valdymo sistemų, ugniasienių, duomenų perdavimo tinklų priežiūrą;

2.6. **eLABa taikomosios programinės įrangos administratorius** – pagrindinio eLABa tvarkytojo paskirtas darbuotojas, vykdantis eLABa taikomosios programinės įrangos priežiūrą;

2.7. **pagrindinis eLABa administratorius** – pagrindinio eLABa tvarkytojo darbuotojas, kuriam tvarkytojas paskyrė pareigą ir teisę koordinuoti visų kitų eLABa administratorių ar paslaugų teikėjo darbą prižiūrint eLABa informacinę sistemą ir (ar) jos infrastruktūrą;

2.8. **vidinis eLABa naudotojas** – eLABa naudotojas, darbo santykiais susijęs su eLABa valdytoju arba eLABa tvarkytoju, vykdantis kitas, nei Saugos nuostatų 2.1–2.7 papunkčiuose aptariamas, eLABa nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose numatytas institucijų funkcijas naudojant eLABa, kitų eLABa naudotojų eLABa duomenų tvarkymą (eLABa naudotojų aptarnavimo, leidinių duomenų registravimo ir kt.).

3. eLABa duomenų saugos užtikrinimo prioritetinės kryptys: saugus eLABa duomenų teikimas eLABa duomenų gavėjams, teisėtas, saugus ir kokybiškas eLABa duomenų tvarkymas bei teisėtas ir saugus jų naudojimas.

4. eLABa elektroninės informacijos saugumo užtikrinimo tikslai:

4.1. eLABa elektroninės informacijos vientisumo, prieinamumo ir konfidencialumo užtikrinimas;

4.2. saugaus duomenų tvarkymo automatiniu būdu sąlygų užtikrinimas.

5. eLABa valdytojas – Lietuvos Respublikos švietimo, mokslo ir sporto ministerija, A. Volano g. 2, LT-01516 Vilnius, kuri:

5.1. koordinuoja Saugos nuostatų, eLABa saugos politiką įgyvendinančių dokumentų rengimą ir kontroliuoja jų įgyvendinimą;

5.2. tvirtina eLABa saugos politiką įgyvendinančius dokumentus;

5.3. sprendžia eLABa funkcijų plėtros klausimus;

5.4. koordinuoja elektroninės informacijos tvarkymo teisėtumo priežiūrą ir užtikrinimą;

5.5. koordinuoja eLABa saugos politikos įgyvendinimą.

6. Pagrindinis eLABa tvarkytojas – Vilniaus universitetas, Universiteto g. 3, LT-01513 Vilnius.

7. Pagrindinio eLABa tvarkytojo saugos tvarkymo ir įgyvendinimo funkcijas Vilniaus universitete atlieka Informacinių technologijų paslaugų centras (adresas – Saulėtekio al. 9, II jungiamieji rūmai, LT-10222, Vilnius), kuris:

7.1. užtikrina nepertraukiamą eLABa veikimą, elektroninės informacijos, saugomos Vilniaus universiteto administruojamose eLABa tarnybinėse stotyse, saugą ir saugų elektroninės informacijos perdavimą kompiuterių tinklais (automatiniu būdu);

7.2. įgyvendina Saugos nuostatuose, eLABa saugos politiką įgyvendinančiuose teisės aktuose nustatytas eLABa duomenų saugaus rinkimo, sisteminimo, saugojimo ir teikimo eLABa duomenų gavėjams organizacines, technines ir kitas priemones;

7.3. teikia eLABa valdytojui siūlymus dėl eLABa saugos politikos įgyvendinimo plėtros, techninių, programinių priemonių įsigijimo, jų modernizavimo, priežiūros ir tobulinimo;

7.4. užtikrina tinkamą eLABa valdytojo priimtų teisės aktų ir rekomendacijų įgyvendinimą;

7.5. skiria eLABa saugos įgaliotinį;

7.6. skiria eLABa pagrindinį administratorių ir kitus eLABa administratorius;

7.7. užtikrina eLABa sąveiką su kitomis informacinėmis sistemomis;

7.8. užtikrina eLABa funkcijų pokyčių įgyvendinimą;

7.9. teikia eLABa valdytojui atitikties bei rizikos vertinimus ir siūlo susijusius veiksmų planus;

7.10. teisės aktų nustatyta tvarka teikia informaciją apie eLABa saugos politikos įgyvendinimą;

7.11. vykdo kitas eLABa saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose nustatytas tvarkytojo funkcijas.

8. Kiti eLABa tvarkytojai ir duomenų valdytojai:

8.1. užtikrina savo valdomos ir tvarkomos eLABa elektroninės informacijos saugą;

8.2. įgyvendina Saugos nuostatuose, eLABa saugos politiką įgyvendinančiuose teisės aktuose nustatytas eLABa duomenų saugaus rinkimo, sisteminimo, saugojimo ir teikimo eLABa duomenų gavėjams organizacines, technines ir kitas priemones;

8.3. teikia pagrindiniam eLABa tvarkytojui siūlymus dėl eLABa saugos politikos įgyvendinimo plėtros, techninių, programinių priemonių įsigijimo, jų modernizavimo, priežiūros ir tobulinimo;

8.4. užtikrina tinkamą eLABa valdytojo priimtų teisės aktų bei rekomendacijų įgyvendinimą savo institucijoje;

8.5. skiria eLABa tvarkytojo arba duomenų valdytojo eLABa saugos įgaliotinį;

8.6. prireikus skiria eLABa tvarkytojo arba duomenų valdytojo eLABa administratorių;

8.7. teisės aktų nustatyta tvarka pagrindiniam eLABa tvarkytojui teikia informaciją apie eLABa saugos politikos įgyvendinimą.

9. Pagrindinio eLABa tvarkytojo eLABa saugos įgaliotinis, įgyvendindamas eLABa saugą, atlieka šias funkcijas:

9.1. teikia pagrindinio eLABa tvarkytojo vadovui siūlymus dėl:

9.1.1. pagrindinio eLABa ir kitų eLABa administratorių paskyrimo ir reikalavimų administratoriams nustatymo;

9.1.2. eLABa saugos dokumentų priėmimo, keitimo ar panaikinimo;

9.1.3. eLABa atitikties saugos reikalavimams įgyvendinimo.

9.2. koordinuoja elektroninės informacijos saugos incidentų, įvykusių eLABa, tyrimą, kai to neatlieka kompiuterinių incidentų tyrimo grupės;

9.3. teikia eLABa administratoriams privalomus vykdyti nurodymus ir pavedimus;

9.4. bendradarbiauja su eLABa tvarkytojų ir duomenų valdytojų eLABa saugos įgaliotiniais, informuoja eLABa tvarkytojus ir eLABa naudotojus apie eLABa saugos problematiką;

9.5. atsako už eLABa saugos politikos įgyvendinimo organizavimą ir peržiūrą;

9.6. organizuoja eLABa saugos mokymus pagrindinio eLABa tvarkytojo vidiniams naudotojams ir administratoriams;

9.7. organizuoja eLABa atitikties organizaciniams ir techniniams reikalavimams ir susijusius rizikos vertinimus;

9.8. atlieka kitas Saugos nuostatuose ir kituose eLABa saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas ir vykdo kitus nurodymus, susijusius su eLABa sauga.

10. eLABa tvarkytojo ar duomenų valdytojo eLABa saugos įgaliotinis, įgyvendindamas eLABa saugą, atlieka šias funkcijas:

10.1. teikia eLABa tvarkytojui ar duomenų valdytojui siūlymus dėl:

10.1.1. eLABa tvarkytojo ar duomenų valdytojo eLABa administratorių paskyrimo;

10.1.2. eLABa tvarkytojo ar duomenų valdytojo eLABa saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

10.1.3. eLABa tvarkytojo ar duomenų valdytojo atitikties eLABa saugos reikalavimams įgyvendinimo;

10.2. bendradarbiauja su pagrindinio eLABa tvarkytojo eLABa saugos įgaliotiniu atliekant elektroninės informacijos saugos incidentų, įvykusių eLABa, tyrimą;

10.3. dalyvauja, atliekant atitikties eLABa organizaciniams ir techniniams reikalavimams ir susijusius rizikos vertinimus;

10.4. teikia eLABa tvarkytojo eLABa administratoriui privalomus vykdyti nurodymus ir pavedimus;

10.5. atlieka eLABa saugos mokymus eLABa tvarkytojo ar duomenų valdytojo vidiniams eLABa naudotojams ir eLABa administratoriams;

10.6. atlieka kitas Saugos nuostatuose ir kituose eLABa saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas ir vykdo kitus nurodymus, susijusius su eLABa sauga.

11. eLABa saugos įgaliotiniai negali atlikti eLABa administratoriaus funkcijų.

12. Pagrindinio eLABa administratoriaus funkcijos:

12.1. teikia privalomus vykdyti nurodymus eLABa sisteminiams, taikomosios programinės įrangos ir pagrindinio eLABa tvarkytojo naudotojų teisių administratoriams;

12.2. eLABa administravimo klausimais bendradarbiauja su kitų eLABa tvarkytojų įgaliotais asmenimis;

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

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

12.5. vykdo kitas tiesiogiai su eLABa administravimu susijusias funkcijas.

13. eLABa taikomosios programinės įrangos administratoriai:

13.1. užtikrina eLABa taikomosios programinės įrangos veikimą;

13.2. vykdo eLABa taikomosios programinės įrangos priežiūrą;

13.3. vykdo paskirtų komponentų ir eLABa naudotojų prieigos teisių administravimą;

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

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

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

13.7. prireikus tvarko ir administruoja visų institucijų paskyrų duomenis;

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

13.9. vykdo kitas tiesiogiai su eLABa administravimu susijusias funkcijas;

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

13.11. testuoja paskirtų komponentų funkcionalumą juos tobulinant ir prižiūrint;

13.12. vykdo pagrindinio eLABa tvarkytojo ir Tvarkytojų eLABa saugos įgaliotinių nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu, ir teikia informaciją apie saugą užtikrinančių pagrindinių eLABa komponentų būklę.

14. eLABa sisteminiai administratoriai atlieka šias funkcijas:

14.1. užtikrina eLABa sisteminės programinės įrangos ir duomenų bazių valdymo programinės įrangos veikimą ir priežiūrą paskirtoje administruoti infrastruktūroje;

14.2. atlieka atsarginių eLABa duomenų kopijų kūrimą, saugojimą, atkūrimą bei sunaikinimą;

14.3. atlieka visiškus ar dalinius duomenų atkūrimo bandymus iš atsarginių eLABa saugomų duomenų kopijų;

14.4. užtikrina eLABa sisteminės programinės įrangos saugą;

14.5. nustato eLABa pažeidžiamas vietas ir informuoja apie jas eLABa saugos įgaliotinį;

14.6. atsako už kompiuterių tinklo ugniasienių konfigūravimą ir priežiūrą;

14.7. atsako už incidentų, dėl kurių buvo prarasti duomenys, priežasčių ir sprendimų ieškojimą, jų protokolavimą ir informuoja eLABa naudotojus apie duomenų atkūrimą po incidento, kurio metu buvo prarasti duomenys;

14.8. vykdo pagrindinio eLABa saugos įgaliotinio nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu.

15. eLABa naudotojų teisių administratorių funkcijos:

15.1. tvarko ir administruoja savo institucijos eLABa klasifikatorius;

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

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

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

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

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

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

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

15.9. vykdo pagrindinio eLABa tvarkytojo ir Tvarkytojo eLABa saugos įgaliotinių ir pagrindinio administratoriaus nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu;

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

16. eLABa lokalaus tinklo ir darbo vietų administratorių funkcijos:

16.1. užtikrina savo institucijos lokalių tinklų veikimą;

16.2. prižiūri savo institucijos lokalius tinklus;

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

16.4. prižiūri eLABa naudotojų kompiuterines darbo vietas savo institucijoje;

16.5. diegia, atnaujina antivirusines programas savo institucijos eLABa naudotojų darbo vietose;

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

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

17. Teisės aktai, kuriais vadovaujamasi tvarkant eLABa duomenis ir užtikrinant jų saugumą:

17.1. 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;

17.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

17.3. Lietuvos Respublikos elektroninių ryšių įstatymas;

17.4. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

17.5. Lietuvos Respublikos kibernetinio saugumo įstatymas;

17.6. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

17.7. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas (toliau – Aprašas), Saugos dokumentų turinio gairių aprašas, Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas (toliau – Svarbos 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“;

17.8. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti 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“;

17.9. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

17.10. Lietuvos mokslo ir studijų institucijų kompiuterių tinklo LITNET naudojimo taisyklės, patvirtintos Lietuvos Respublikos švietimo ir mokslo ministro 2011 m. liepos 18 d. įsakymu Nr. V-1348 „Dėl Lietuvos mokslo ir studijų institucijų kompiuterių tinklo LITNET paslaugų teikimo tvarkos aprašo ir Lietuvos mokslo ir studijų institucijų kompiuterių tinklo LITNET naudojimo taisyklių patvirtinimo“;

17.11. Lietuvos Respublikos švietimo ir mokslo ministro 2006 m. liepos 14 d. įsakymas Nr. ISAK-1506 „Dėl Lietuvos akademinės elektroninės bibliotekos informacinės sistemos nuostatų ir Lietuvos akademinės elektroninės bibliotekos informacinės sistemos duomenų saugos nuostatų patvirtinimo“;

17.12. Lietuvos Respublikos švietimo ir mokslo ministro 2015 m. liepos 2 d. įsakymas Nr. V-710 „Dėl Lietuvos akademinės elektroninės bibliotekos informacinės sistemos saugos politiką įgyvendinančių dokumentų patvirtinimo“;

17.13. Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatai, patvirtinti Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“ (toliau – Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatai).

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

18. Vadovaujantis Svarbos gairių aprašo 9.1 ir 9.3 papunkčiais eLABa tvarkoma elektroninė informacija priskiriama vidutinės svarbos informacijos kategorijai.

19. Vadovaujantis Svarbos gairių aprašo 12.3 papunkčiu, eLABa priskiriama trečiajai informacinės sistemos kategorijai.

20. Pagrindinio eLABa tvarkytojo eLABa saugos įgaliotinis, atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja eLABa rizikos įvertinimą.

21. Prireikus pagrindinio eLABa tvarkytojo eLABa saugos įgaliotinis gali organizuoti neeilinį eLABa (ar jos sudedamųjų dalių) rizikos įvertinimą.

22. eLABa rizikos rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kurią pagrindinio eLABa tvarkytojo eLABa saugos įgaliotinis pateikia pagrindinio eLABa tvarkytojo vadovui.

23. Rizikos įvertinimo ataskaita rengiama įvertinant rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus.

24. Svarbiausi rizikos veiksniai eLABa duomenims, programinei, techninei įrangai yra:

24.1. subjektyvūs netyčiniai veiksniai (duomenų tvarkymo klaidos, klaidingų duomenų teikimas, duomenų perdavimo tinklais sutrikimai, programinės įrangos klaidos ir kita);

24.2. subjektyvūs tyčiniai veiksniai (nesankcionuotas naudojimasis informacine sistema, siekiant gauti duomenų, duomenų keitimas, naikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, vagystės ir kita);

24.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

25. Pagrindiniai eLABa duomenų saugos priemonių parinkimo principai yra šie:

25.1. Lietuvos Respublikos įstatymų ir kitų teisės aktų nuostatos ir saugomi gėriai vienodai taikomi tiek fizinėje, tiek kibernetinėje erdvėje;

25.2. taikomos kibernetinio saugumo užtikrinimo priemonės negali būti griežtesnės, negu būtina kibernetiniam saugumui užtikrinti, o taikomi teisiniai, organizaciniai ir techniniai kibernetinio saugumo reikalavimai neturi apriboti kibernetinio saugumo dalyvių veiklos kibernetinėje erdvėje labiau negu tai būtina;

25.3. naudojamos kibernetinio saugumo užtikrinimo priemonės pirmiausia turi užtikrinti viešojo intereso apsaugą, tačiau neturi iš esmės pažeisti atskirų vartotojų teisių ar neproporcingai apriboti jų laisvės kibernetinėje erdvėje;

25.4. likutinė rizika turi būti sumažinama iki eLABa saugos politiką įgyvendinančiuose dokumentuose numatytų reikalavimų atitikties lygio;

25.5. duomenų saugos priemonės diegimo kaina turi būti adekvati saugomų duomenų vertei;

25.6. kur galima, turi būti įdiegiamos prevencinės, detekcinės ir korekcinės duomenų saugos priemonės;

25.7. šie principai turi būti derinami tarpusavyje, nė vienam iš jų iš anksto nesuteikiama pirmenybė.

26. Atsižvelgdamas į rizikos įvertinimo ataskaitą, eLABa valdytojas prireikus tvirtina rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

27. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas eLABa valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti per Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemą Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

28. Siekiant užtikrinti Saugos nuostatuose ir kituose eLABa saugos politiką įgyvendinančiuose teisės aktuose išdėstytų nuostatų įgyvendinimo kontrolę, pagrindinis eLABa saugos įgaliotinis ne

rečiau kaip kartą per metus, vadovaudamasis Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“, organizuoja eLABa saugos atitikties vertinimą.

29. Atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama eLABa tvarkytojo vadovui, ir pastebėtų trūkumų šalinimo planas, kurį rengia, tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato eLABa valdytojo vadovas.

30. Informacinių technologijų saugos atitikties vertinimo ataskaitas, pastebėtų trūkumų šalinimo plano kopijas eLABa valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti per Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemą Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

31. eLABa saugos dokumentai turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per metus. eLABa saugos dokumentai taip pat turi būti persvarstomi (peržiūrimi) po to, kai atliekamas rizikos įvertinimas ar informacinių technologijų saugos atitikties vertinimas, arba įvyksta esminių organizacinių, sisteminių ar kitokių pokyčių. Keičiami eLABa saugos dokumentai derinami su krašto apsaugos ministro įgaliota institucija, įgyvendinančia valstybės informacinių išteklių saugos politiką, Aprašo nustatyta tvarka. Keičiami eLABa saugos dokumentai su krašto apsaugos ministro įgaliota institucija, įgyvendinančia valstybės informacinių išteklių saugos politiką, gali būti nederinami tais atvejais, kai atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar saugos politikos nekeičiantys pakeitimai arba taisoma teisės technika.

32. Patvirtintų eLABa saugos politiką įgyvendinančių dokumentų ir jų pakeitimų kopijas eLABa valdytojas ne vėliau kaip per 5 darbo dienas nuo jų patvirtinimo turi pateikti per Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemą Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

33. Programinės įrangos, skirtos apsaugoti eLABa nuo virusų ir kitos kenksmingos programinės įrangos, naudojimo nuostatos:

33.1. visuose eLABa vidaus naudotojų darbo vietų kompiuteriuose ir tarnybinėse stotyse turi būti įdiegiama apsaugos nuo virusų ir kitos nepageidaujamos programinės įrangos sistema;

33.2. apsaugos nuo virusų ir kitos nepageidaujamos programinės įrangos sistema turi tikrinti, ar nėra atnaujinimų bent kartą per 5 paras;

33.3. apsaugos nuo virusų ir kitos nepageidaujamos programinės įrangos sistemai nustačius, jog atnaujinimai yra prieinami – jie turi būti įdiegiami;

33.4. eLABa naudotojų darbo vietose draudžiama naudoti programinę įrangą, galinčią kelti grėsmę eLABa duomenų saugumui.

34. eLABa tvarkytojai turi teisę riboti naudotojų, trikdančių kitų naudotojų prieigą, sistemos darbą, ar naudojančių programinę įrangą, galinčią kelti grėsmę eLABa duomenų saugumui.

35. Pagrindinės kompiuterių tinklo filtravimo įrangos nuostatos:

35.1. į eLABa vidinį tinklą duomenų srautas turi būti praleidžiamas tik eLABa funkcionalumui užtikrinti būtinais protokolais;

35.2. eLABa duomenų perdavimo tinklas nuo viešojo kompiuterių tinklo turi būti atskirtas ugniasiene, kuri palaikytų funkcionalumą filtravimo failų lygmeniu.

36. Leistinos kompiuterių naudojimo ribos ir nuostatos:

36.1. prieigai prie eLABa gali būti naudojami nešiojamieji kompiuteriai ir mobilieji įrenginiai;

36.2. prieigai prie eLABa naudojami kompiuteriai gali būti naudojami ir kitoms eLABa naudotojo ir eLABa administratoriaus funkcijoms atlikti;

36.3. eLABa administratorių tvarkomi eLABa naudotojų asmens duomenys nešiojamuosiuose kompiuteriuose turi būti saugomi tik šifruoti;

36.4. eLABa administratorių naudojami nešiojamieji kompiuteriai turi būti apsaugoti papildomomis fizinės apsaugos priemonėmis bei naudoti papildomas tapatybės nustatymo priemones;

36.5. nepriklausomai nuo tinklo prieigos operatoriaus pasirinkimo, eLABa naudotojams taikomos ir Lietuvos mokslo ir studijų institucijų kompiuterių tinklo LITNET naudojimo taisyklės, patvirtintos Lietuvos Respublikos švietimo ir mokslo ministro 2011 m. liepos 18 d. įsakymu Nr. V-1348 „Dėl Lietuvos mokslo ir studijų institucijų kompiuterių tinklo LITNET paslaugų teikimo tvarkos aprašo ir Lietuvos mokslo ir studijų institucijų kompiuterių tinklo LITNET naudojimo taisyklių patvirtinimo“;

36.6. eLABa administravimui negali būti naudojami mobilūs įrenginiai;

36.7. eLABa administratoriai gali dirbti tik iš nustatytų leistinų IP adresų.

37. Saugaus eLABa elektroninės informacijos gavimo ir teikimo užtikrinimo metodai ir priemonės bei reikalavimai duomenų teikimo sutartims nustatomi Lietuvos akademinės elektroninės bibliotekos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse ir Lietuvos akademinės elektroninės bibliotekos informacinės sistemos naudotojų administravimo taisyklėse, patvirtintose Lietuvos Respublikos švietimo ir mokslo ministro 2015 m. liepos 2 d. įsakymu Nr. V-710 „Dėl Lietuvos akademinės elektroninės bibliotekos informacinės sistemos saugos politiką įgyvendinančių dokumentų patvirtinimo“.

38. Pagrindiniai organizaciniai-techniniai eLABa duomenų atsarginių kopijų darymo, saugojimo ir atkūrimo saugos reikalavimai:

38.1. priimtinas eLABa valdytojui prarastų duomenų kiekis – 8 valandos;

38.2. paskirti eLABa tvarkytojo darbuotojai, atsakingi už eLABa kopijų darymą, saugojimą ir atkūrimą;

38.3. kiekvienas eLABa elektroninės informacijos kopijų darymo ir atstatymo faktas turi būti užregistruotas;

38.4. atsarginės kopijos saugomos kitose patalpose nei darbinės duomenų kopijos;

38.5. eLABa duomenų atkūrimo bandymai atliekami ne rečiau kaip kartą per metus;

38.6. eLABa laikmenos saugomos taip, kad kilus elektroninės informacijos saugos incidentui eLABa veiklą rezerviniame duomenų centre galima būtų atkurti per 2 (dvi) darbo dienas.

39. eLABa duomenų atsarginių kopijų darymo, saugojimo ir atkūrimo tvarkos ir instrukcijos turi būti peržiūrimos ne rečiau kaip kartą per metus.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

40. Pagrindinio eLABa tvarkytojo ir kitų eLABa tvarkytojų saugos įgaliotiniai ir administratoriai negali būti skiriami ar eiti pareigų, jei turi 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 nuobaudos paskyrimo praėję mažiau kaip vieni metai.

41. Pagrindinio eLABa tvarkytojo ir Tvarkytojų eLABa saugos įgaliotiniai privalo išmanyti informacijos saugos užtikrinimo principus ir savo darbe vadovautis Saugos nuostatais, Lietuvos akademinės elektroninės bibliotekos informacinės sistemos nuostatais, patvirtintais Lietuvos Respublikos švietimo ir mokslo ministro 2006 m. liepos 14 d. įsakymu Nr. ISAK-1506 „Dėl Lietuvos

akademinės elektroninės bibliotekos informacinės sistemos nuostatų ir Lietuvos akademinės elektroninės bibliotekos informacinės sistemos duomenų saugos nuostatų patvirtinimo“ (toliau – eLABa nuostatai), eLABa saugos politiką įgyvendinančiais dokumentais, Lietuvos standartais ir kitais teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą.

42. eLABa administratorius turi išmanyti darbą kompiuteriais, operacinėmis sistemomis, taikomosiomis programų sistemomis, kompiuteriniais tinklais, mokėti užtikrinti jų saugumą, taip pat turi išmanyti duomenų bazių administravimą, priežiūrą, būti susipažinęs su Saugos nuostatais, eLABa nuostatais, eLABa saugos politiką įgyvendinančiais dokumentais.

43. Visi eLABa tvarkytojų ir duomenų valdytojų darbuotojai – eLABa vidiniai naudotojai, prieš suteikiant prieigą, privalo turėti pagrindinius darbo kompiuteriu įgūdžius ir turi būti susipažinę su Saugos nuostatais, eLABa saugos politiką įgyvendinančiais dokumentais ir atsakomybe už jų nesilaikymą bei įsipareigoję laikytis jų reikalavimų.

44. Informacinės sistemos saugos mokymų planavimo, organizavimo ir vykdymo tvarka:

44.1. informacinės sistemos vidiniai naudotojai ir administratoriai periodiškai (ne rečiau, kaip kartą per metus) įvairiomis priemonėmis informuojami apie saugumo problematiką (pvz., priminimai elektroniniu paštu, atmintinės ir pan.);

44.2. pirminį informacinės sistemos administratorių duomenų saugos instruktažą, prieš suteikiant prieigos teises, atlieka pagrindinio eLABa tvarkytojo naudotojų teisių administratorius;

44.3. pakartotinis informacinės sistemos administratorių supažindinimas (instruktažas) su duomenų saugos reikalavimais vykdomas atnaujinus saugos dokumentus, išskyrus tais atvejais, kai atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar saugos politikos nekeičiantys pakeitimai arba taisoma teisės technika;

44.4. mokymus tvarkytojo vidiniams naudotojams turi vykdyti tvarkytojo eLABa saugos įgaliotinis ar kitas darbuotojas, išmanantis elektroninės informacijos saugos užtikrinimo principus, arba elektroninės informacijos saugos mokymų paslaugų teikėjas.

V SKYRIUS
eLABa NAUDOTOJŲ SUPAŽINDINIMO SU eLABa SAUGOS DOKUMENTAIS PRINCIPAI

45. eLABa saugos įgaliotiniai, administratoriai ir vidiniai naudotojai su Saugos nuostatais, eLABa saugos politiką įgyvendinančiais dokumentais, kitais teisės aktais, kuriais vadovaujamasi tvarkant eLABa duomenis ir užtikrinant jų saugumą, bei atsakomybe už juose numatytų reikalavimų pažeidimus, supažindinami būdu, užtikrinančiu atsekamumą.

46. Pakartotinai eLABa naudotojai su Saugos nuostatais bei eLABa saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais supažindinami tik tada, kai šie iš esmės pasikeičia. Informacija apie pokyčius eLABa saugos politiką įgyvendinančiuose teisės aktuose siunčiama elektroniniu būdu.

47. eLABa naudotojai, pažeidę Saugos nuostatų ar eLABa saugos politiką įgyvendinančių dokumentų reikalavimus, atsako Lietuvos Respublikos įstatymų ir kitų teisės aktų nustatyta tvarka.

_____