Suvestinė redakcija nuo 2019-10-15

Įsakymas paskelbtas: TAR 2015-07-07, i. k. 2015-11020

LIETUVOS RESPUBLIKOS ŠVIETIMO IR MOKSLO MINISTRAS

ĮSAKYMAS DĖL LIETUVOS AKADEMINĖS ELEKTRONINĖS BIBLIOTEKOS INFORMACINĖS SISTEMOS SAUGOS POLITIKĄ ĮGYVENDINANČIŲ DOKUMENTŲ PATVIRTINIMO

2015 m. liepos 2 d. Nr. V-710
Vilnius

Vadovaudamasi 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 8 punktu:

1. T v i r t i n u pridedamus:

1.1. Lietuvos akademinės elektroninės bibliotekos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisykles;

1.2. Lietuvos akademinės elektroninės bibliotekos informacinės sistemos veiklos tęstinumo valdymo planą;

1.3. Lietuvos akademinės elektroninės bibliotekos informacinės sistemos naudotojų administravimo taisykles.

2. P a v e d u Lietuvos akademinės elektroninės bibliotekos informacinės sistemos (toliau – eLABa) techniniams centrams parengti ir pagrindiniam eLABa tvarkytojui Vilniaus universitetui iki 2015 m. rugsėjo 30 dienos patvirtinti:

2.1. eLABa veiklos tęstinumo rizikos mažinimo prevencinių priemonių aprašus;

2.2. eLABa veiklos tęstinumo valdymo ir atkūrimo grupių sudėtį;

2.3. eLABa įrangos, būtinos atkurti eLABa infrastruktūrą minimalia ir visa apimtimi, sąmatas;

2.4. eLABa duomenų teikimo bei kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių (jei tokios sutartys sudarytos) sąrašą;

2.5. eLABa duomenų atkūrimo iš atsarginių kopijų tvarkos aprašą.

Švietimo ir mokslo ministrė Audronė Pitrėnienė

SUDERINTA

Lietuvos Respublikos vidaus reikalų ministerijos
2015 m. birželio 2 d. raštu Nr. 1D-4962

PATVIRTINTA
Lietuvos Respublikos švietimo ir mokslo ministro
2015 m. liepos 2 d. įsakymu Nr. V-710
(Lietuvos Respublikos švietimo, mokslo ir sporto ministro
2019 m. spalio 14 d. įsakymo Nr. V-1150
redakcija)

LIETUVOS AKADEMINĖS ELEKTRONINĖS BIBLIOTEKOS INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos akademinės elektroninės bibliotekos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) nustato tvarką, pagal kurią turi būti saugiai tvarkoma Lietuvos akademinės elektroninės bibliotekos informacinės sistemos (toliau – eLABa) elektroninė informacija.

2. Taisyklės privalomos eLABa naudotojams ir administratoriams.

3. Už Taisyklių įgyvendinimo organizavimą ir kontrolę atsako pagrindinio eLABa tvarkytojo eLABa saugos įgaliotinis bendrai ir eLABa naudojančių institucijų saugos įgaliotiniai subsidiariai.

4. 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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, Lietuvos akademinės elektroninės bibliotekos informacinės sistemos nuostatais, (toliau – eLABa nuostatai) ir Lietuvos akademinės elektroninės bibliotekos informacinės sistemos duomenų saugos nuostatais (toliau – eLABa duomenų saugos nuostatai), 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“, 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“, ir kitais teisės aktais.

5. Taisyklėse vartojamos sąvokos suprantamos taip, kaip apibrėžtos Bendruosiuose elektroninės informacijos saugos reikalavimuose, Saugos dokumentų turinio gairių apraše, patvirtintame 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“, eLABa nuostatuose, eLABa duomenų saugos nuostatuose ir kituose saugų duomenų tvarkymą reglamentuojančiuose teisės aktuose.

6. eLABa informacinėje sistemoje tvarkoma eLABa elektroninė informacija yra pateikta eLABa nuostatų 19 punkte.

7. eLABa pagal tvarkomą informaciją priskirta informacinės sistemos kategorijai, kuri nurodyta eLABa duomenų saugos nuostatų 19 punkte.

8. Už eLABa elektroninės informacijos tvarkymą atsakingi:

8.1. eLABa administratoriai – už informacijos, nurodytos eLABa nuostatų 19.2, 19.5, 19.7, 19.8, 19.9, 19.10 papunkčiuose;

8.2. vidiniai eLABa naudotojai (darbo vadovai, bibliotekininkai, institucijos padalinio registratoriai, institucijos registratoriai) – už informacijos, nurodytos eLABa nuostatų 19.1, 19.2, 19.3, 19.4, 19.6 papunkčiuose;

8.3. eLABa naudotojai už:

8.3.1. tik savo duomenis eLABa nuostatų 19.3 papunktyje;

8.3.2. tik savo duomenis eLABa nuostatų 19.4 papunktyje.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

9. Kompiuterinės įrangos saugos priemonės:

9.1. eLABa administratorių kompiuteriuose turi būti naudojama antivirusinė ir kita programinė įranga, skirta aptikti ir realiu metu stebėti ir šalinti kenksmingą programinę įrangą. Ši įranga turi būti nuolatos, bet ne rečiau kaip kartą per savaitę, atnaujinama ir automatiškai turi informuoti lokalaus darbo vietos administratorių apie tai, kurių eLABa posistemių, funkciškai savarankiškų sudedamųjų dalių uždelsta atsinaujinimo veikla;

9.2. turi būti operatyviai išbandomi ir įdiegiami eLABa administratorių darbo vietų kompiuterinės įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai; eLABa lokalaus tinklo ir darbo vietų administratorius reguliariai, ne rečiau kaip kartą per mėnesį, turi įvertinti informaciją apie eLABa vidinių naudotojų darbo vietų kompiuterinėje įrangoje neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumo svarbos lygius;

9.3. eLABa administratorių kompiuterinėje įrangoje turi būti naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga;

9.4. eLABa administratorių darbo vietose gali būti naudojamos tik tarnybinėms reikmėms skirtos išorinės duomenų laikmenos (pavyzdžiui, USB, CD / DVD ir kt.); šios laikmenos negali būti naudojamos veiklai, nesusijusiai su teisėtu eLABa tvarkymu;

9.5. nuotolinis prisijungimas prie eLABa turi būti vykdomas protokolu, skirtu duomenims šifruoti.

10. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

10.1. neatliekant jokių veiksmų su eLABa 30 minučių, eLABa taikomoji programinė įranga turi užsirakinti, kad toliau naudotis eLABa galima būtų, tik pakartotinai patvirtinus savo tapatybę;

10.2. techninių centrų eLABa tarnybinėse stotyse turi būti naudojama antivirusinė ir kita programinė įranga, skirta aptikti ir realiu metu stebėti ir šalinti kenksmingą programinę įrangą. Ši įranga turi būti nuolatos, bet ne rečiau kaip kartą per savaitę atnaujinama ir automatiškai turi informuoti eLABa sisteminį administratorių apie tai, kurių eLABa posistemių, funkciškai savarankiškų sudedamųjų dalių uždelsta atsinaujinimo veikla; eLABa komponentai be kenksmingos programinės įrangos aptikimo priemonių gali būti eksploatuojami, jeigu rizikos vertinimo metu yra patvirtinama, kad šių komponentų rizika yra priimtina;

10.3. turi būti operatyviai išbandomi ir įdiegiami eLABa tarnybinių stočių įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai; techninių centrų eLABa administratoriai reguliariai, ne rečiau kaip kartą per savaitę, turi įvertinti informaciją apie eLABa posistemėms, funkciškai savarankiškoms sudedamosioms dalims neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumo svarbos lygius;

10.4. eLABa dalys, patvirtinančios naudotojo tapatumą, turi drausti išsaugoti slaptažodžius;

10.5. eLABa vidinių naudotojų ir administratorių darbo vietose bei tarnybinėse stotyse naudojama tik legali, pripažinta tinkama programinė įranga;

10.6. eLABa techninė ir programinė įranga turi būti prižiūrima, laikantis gamintojo rekomendacijų;

10.7. eLABa techninės ir programinės įrangos priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai;

10.8. eLABa sisteminis administratorius turi būti įspėjamas, kai pagrindinėje eLABa kompiuterinėje įrangoje sumažėja iki nustatytos pavojingos ribos laisvos kompiuterio atminties ar vietos diske, ilgai stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja;

10.9. eLABa turi turėti įvestos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemones;

10.10. svarbiausia įranga turi būti dubliuojama ir jos techninė būklė nuolat stebima;

10.11. informacija apie į eLABa įrašomus duomenis, apie eLABa įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis į eLABa, visus eLABa naudotojų vykdomus veiksmus, kitus saugai svarbius įvykius, nurodant eLABa naudotojo identifikatorių ir elektroninės informacijos saugai svarbaus įvykio ar vykdyto veiksmo laiką, turi būti saugoma ne trumpiau kaip 6 mėnesius. Šie duomenys turi būti saugomi ne toje pačioje informacinėje sistemoje, kurioje jie įrašomi, taip pat jie turi būti analizuojami ne rečiau kaip kartą per savaitę;

10.12. pagrindinėse eLABa tarnybinėse stotyse turi būti naudojamos vykdomo kodo kontrolės priemonės, automatiškai apribojančios ar informuojančios apie neautorizuoto programinio kodo vykdymą;

10.13. pagrindinėse eLABa tarnybinėse stotyse turi būti įjungtos ugniasienės, sukonfigūruotos praleisti tik su eLABa funkcionalumu ir administravimu susijusį duomenų srautą;

10.14. programinės įrangos bandymas atliekamas, naudojant atskirą testavimo aplinką, kurioje nėra saugomi asmens duomenys;

10.15. kiekvienas eLABa naudotojas turi būti informacinėje sistemoje unikaliai identifikuojamas eLABa naudotojo vardu. Asmens kodas negali būti naudojamas kaip eLABa naudotojo identifikatorius;

10.16. eLABa naudotojai ir eLABa administratoriai turi patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone;

10.17. eLABa naudotojų tapatumui patvirtinti gali būti naudojamos dviejų veiksnių tapatumo patvirtinimo priemonės.

11. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

11.1. eLABa tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių eLABa naudotojų kompiuterinę įrangą nuo kenksmingo kodo;

11.2. viešaisiais ryšių tinklais perduodamos eLABa elektroninės informacijos konfidencialumas turi būti užtikrintas, naudojant šifravimą, virtualų privatų tinklą (angl. *virtual private network*), skirtines linijas, saugų elektroninių ryšių tinklą ar kitas priemones;

11.3. duomenų perdavimo tinklo mazgai ir ryšio linijos turi būti dubliuoti ir jų techninė būklė nuolat stebima;

11.4. eLABa tinkle turi būti įdiegtos ir veikti automatinės įsilaužimo aptikimo sistemos. Įsilaužimo aptikimo konfigūracijos ir kibernetinių incidentų aptikimo taisyklės turi būti saugomos elektronine forma atskirai nuo valstybės informacinės infrastruktūros techninės įrangos (kartu nurodant įgyvendinimo, atnaujinimo ir datas, atsakingus asmenis, taikymo periodus);

11.5. ne rečiau kaip kartą per mėnesį yra atliekama saugasienių užfiksuotų įvykių analizė ir pastebėtos neatitiktys saugumo reikalavimams šalinamos.

12. Tarnybinių stočių patalpų ir aplinkos saugumo užtikrinimo priemonės:

12.1. eLABa tarnybinių stočių patalpos turi būti apsaugotos nuo neteisėto asmenų patekimo į jas;

12.2. eLABa tarnybinių stočių patalpose turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir (arba) apsaugos tarnybos stebėjimo pulto;

12.3. svarbiausia kompiuterinė įranga ir duomenų perdavimo tinklo mazgai turi turėti rezervinį maitinimo šaltinį, užtikrinantį šios įrangos veikimą ne mažiau kaip 30 min.;

12.4. eLABa tarnybinių stočių patalpose turi būti oro kondicionavimo ir drėgmės kontrolės įranga;

12.5. visose patalpose, kuriose yra eLABa tarnybinių stočių techninė įranga, turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų;

12.6. patekimas prie vidinių eLABa naudotojų darbo vietų turi būti kontroliuojamas;

12.7. įrengta elektroninė patalpų perimetro kontrolės sistema. Tarnybinių stočių patalpos turi atskirą elektroninę perimetro kontrolės sistemą;

12.8. įrengta tam tikrų patalpų apsaugos signalizacija, kurios signalai, pasibaigus darbo dienai, taip pat poilsio ir švenčių dienomis persiunčiami patalpas saugančiai tarnybai;

12.9. eLABa sisteminiam administratoriui išduodama asmeninė magnetinė įėjimo kortelė, kurią įeidamas ir išeidamas pasižymi patikros punktuose;

12.10. visi eLABa sisteminio administratoriaus ir kitų darbuotojų įėjimų ir išėjimų į patalpas kartai fiksuojami ir laikomi elektronine forma ne trumpiau kaip 1 metus;

12.11. kiti darbuotojai, kuriems nėra išduota asmeninė magnetinė įėjimo kortelė, į patalpas gali patekti tik lydimi už atitinkamo techninio centro patalpų kontrolę atsakingo asmens;

12.12. įvykus apsaugos sistemos gedimui, pildomas įėjimo punkto žurnalas, nurodant patekimo priežastį, pradžią ir pabaigą;

12.13. įėjimo punkto žurnalas privalo būti pateiktas, eLABa saugos įgaliotiniui pareikalavus;

12.14. lankytojams ir svečiams privaloma atsakingo darbuotojo palyda;

12.15. lankytojai ir svečiai pasirašo įėjimo punkto žurnale. Už apsilankymą atsakingas darbuotojas patvirtina apsilankymo duomenis ir pasirašo įėjimo punkto žurnale;

12.16. po 22 val. ir ne darbo dienomis į atitinkamo techninio centro patalpas savarankiškai patekti gali tik eLABa sisteminis administratorius, eLABa saugos įgaliotinis ir kiti specialius leidimus turintys darbuotojai, kuriuos patvirtina atitinkamo techninio centro vadovas;

12.17. prieš patekdamas į patalpas po 22 val. ir ne darbo dienomis, darbuotojas privalo informuoti saugos tarnybą (apsaugos darbuotoją).

13. Belaidžio tinklo saugumas ir kontrolė informacinės sistemos tvarkytojų patalpose:

13.1. leidžiama naudoti tik su institucijos saugos įgaliotiniu suderintus belaidžio tinklo įrenginius (belaidės prieigos taškus), atitinkančius techninius kibernetinio saugumo reikalavimus;

13.2. tikrinami prieigai prie eLABa naudojami belaidžiai įrenginiai, eLABa tvarkytojo eLABa saugos įgaliotiniui arba atitinkamai savo institucijos saugos įgaliotiniui pranešama apie neleistinus ar techninių kibernetinio saugumo reikalavimų neatitinkančius belaidžius įrenginius;

13.3. suderinus su eLABa tvarkytojo eLABa saugos įgaliotiniu arba atitinkamai savo institucijos saugos įgaliotiniu, belaidės prieigos taškai gali būti diegiami tik atskirame potinklyje, kontroliuojamoje zonoje;

13.4. prisijungiant prie belaidžio tinklo, turi būti taikomas naudotojų tapatumo patvirtinimo EAP (angl. Extensible Authentication Protocol) / TLS (angl. Transport Layer Security) protokolas;

13.5. belaidėje sąsajoje turi būti išjungtas tinklo stebėsenos ir valdymo protokolas (SNMP);

13.6. turi būti išjungti visi nebūtini valdymo protokolai;

13.7. turi būti išjungti nenaudojami duomenų perdavimo TCP (angl. Transmission Control Protocol) / UDP (angl. User Datagram Protocol) protokolų naudojami prievadai;

13.8. turi būti išjungtas lygiarangis (angl. peer to peer) funkcionalumas, leidžiantis belaidžiais įrenginiais tarpusavyje palaikyti ryšį;

13.9. belaidis ryšys turi būti šifruojamas mažiausiai 256 bitų ilgio raktu;

13.10. prieš pradedant naudoti belaidę prieigos stotelę ir šifruoti belaidį ryšį, turi būti pakeisti belaidės prieigos stotelėje standartiniai gamintojo slaptažodžiai ir šifravimo raktai.

14. eLABa naudojamų svetainių, pasiekiamų iš viešųjų elektroninių ryšių tinklų, saugumas ir kontrolė:

14.1. svetainės, patvirtinančios nuotolinio prisijungimo tapatumą, turi drausti automatiškai išsaugoti slaptažodžius;

14.2. draudžiama slaptažodžius saugoti programiniame kode;

14.3. turi būti įgyvendinti svetainės kriptografijos reikalavimai:

14.3.1. svetainės administravimo darbai turi būti atliekami per šifruotą ryšio kanalą, šifruojant ne trumpesniu kaip 256 bitų raktu;

14.3.2. šifruojant naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų; sertifikato raktas turi būti ne trumpesnis kaip 1024 bitų;

14.3.3. svetainės kriptografinės funkcijos turi būti įdiegtos tarnybinės stoties, kurioje yra svetainė, dalyje arba kriptografiniame saugumo modulyje (angl. Hardware security module);

14.4. draudžiama tarnybinėje stotyje saugoti sesijos duomenis (identifikatorių), pasibaigus susijungimo sesijai;

14.5. turi būti naudojama svetainės naudotojo įvedamų duomenų tikslumo kontrolė (angl. Validation);

14.6. tarnybinė stotis, kurioje yra svetainė, neturi rodyti svetainės naudotojui klaidų pranešimų apie svetainės programinį kodą ar tarnybinę stotį;

14.7. tarnybinė stotis, kurioje yra svetainė, turi leisti tik svetainės funkcionalumui užtikrinti reikalingus HTTP metodus;

14.8. turi būti uždrausta naršyti svetainės aplankuose (angl. Directory browsing).

15. Technologinio pažeidžiamumo valdymas:

15.1. ne rečiau kaip kartą į metus pagrindinio eLABa tvarkytojo eLABa saugos įgaliotinis organizuoja grėsmių ir pažeidžiamumų, galinčių turėti įtakos eLABa kibernetiniam saugumui, vertinimą kartu su rizikos vertinimu ir (arba) informacinių technologijų saugos atitikties vertinimu;

15.2. pažeidžiamumų nustatymo planas parengiamas eLABa rizikos vertinimo pradžioje, nustatant rizikos vertinimo apimtį. Pažeidžiamumų nustatymo planas turi apimti pažeidžiamumų nustatymo būdą (ar bus atliekamas savo jėgomis, ar perkamos išorinių paslaugų teikėjų paslaugos) ir apimtį, pažeidžiamumo nustatymo dalyvius, jų teises ir pareigas;

15.3. technologinių pažeidžiamumų įvertinimas turi būti atliekamas pagal viešai žinomą ir pripažintą atvirą ar komercinę pažeidžiamumų įvertinimo metodiką (angl. penetration testing methodology);

15.4. technologinių pažeidžiamumų įvertinimo būdus, metodus ir priemones, įskaitant naudojamą pažeidžiamumų nustatymo programinę įrangą, paslaugų teikėjas turi suderinti su pagrindinio eLABa tvarkytojo eLABa saugos įgaliotiniu prieš pradedant eLABa technologinių pažeidžiamumų įvertinimą;

15.5. atliekant technologinių pažeidžiamumų įvertinimą savo jėgomis, naudojama speciali pažeidžiamumų nustatymo programinė įranga „Nessus“;

15.6. technologinių pažeidžiamumų testavimo rezultatai klasifikuojami, suteikiant pažeidžiamumui kritiškumo balą, atsižvelgiant į jo įtaką, išnaudojimo sudėtingumą ir tikimybę. Kritiškumo balas suteikiamas priklausomai nuo naudojamo pažeidžiamumų testavimo būdo ir naudojamos metodikos: atliekant pažeidžiamumų testavimą su specialia programine įranga, pažeidžiamumai vertinami vadovaujantis CVSS (angl. Common Vulnerability Scoring System) metodika, o rankiniu būdu – 5 balų skalėje, kad būtų galima susieti su rizikos vertinimo kriterijais, naudojamais Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemoje (ARSIS). Bendro rizikos vertinimo metu, vertinant grėsmių tikimybes, atsižvelgiama į technologinio pažeidžiamumų įvertinimo rezultatus;

15.7. atlikus įvertinimą rengiama detali atlikto technologinio pažeidžiamumų testavimo rezultatų ataskaita techniniams specialistams;

15.8. ataskaitoje technologinio pažeidžiamumų testavimo rezultatai pateikiami tokioje struktūroje:

15.8.1. testo numeris ir pavadinimas;

15.8.2. testo / atakos paskirtis, siekiamas tikslas ir trumpas aprašymas;

15.8.3. testo objektai, taikiniai (IP adresai, prievadų numeriai, atakuoti URL parametrai, atakuotų žiniatinklio formų parametrai ir kt.);

15.8.4. testui / atakai naudoti programiniai / aparatiniai įrankiai ir priemonės;

15.8.5. testo / atakos turinys, parašas, naudoto kenksmingo programinio kodo išeities tekstas, žiniatinklio užklausų parametrų reikšmės ir kt.;

15.8.6. testo rezultatas (sėkmingas, nesėkmingas);

15.8.7. testo ar testavimo įrankio išdavos (angl. output) ir pažeidžiamumo buvimo/nebuvimo įrodymai;

15.8.8. testo rezultatai, išvados, pažeidžiamumo pašalinimo rekomendacijos, šalinimo planas;

15.9. kartu su technologinių pažeidžiamumų įvertinimu, turi būti atliktas kibernetinių atakų imitavimas. Kibernetinių atakų scenarijai parengiami pažeidžiamumų nustatymo plano sudarymo metu arba paslaugų teikėjui derinant technologinių pažeidžiamumų įvertinimo metodiką.

16. Kitos priemonės, naudojamos eLABa elektroninės informacijos saugai užtikrinti:

16.1. turi būti registruojami duomenų bazių struktūros ir tarnybinių stočių operacinės sistemos pakeitimai;

16.2. baigęs darbą, eLABa naudotojas turi užtikrinti, kad su eLABa elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungti nuo eLABa, uždaryti programinę įrangą, įjungti ekrano užsklandą su slaptažodžiu;

16.3. eLABa veikla atkuriama, vadovaujantis Lietuvos akademinės elektroninės bibliotekos informacinės sistemos veiklos tęstinumo valdymo planu.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

17. Saugaus elektroninės informacijos keitimo, atnaujinimo, įvedimo ir naikinimo užtikrinimo tvarka:

17.1. tvarkomus duomenis įvesti, atnaujinti, šalinti gali eLABa naudotojas pagal jam priskirtą vaidmenį sistemoje, nurodytą Taisyklių 8 punkte;

17.2. pateikiamų į eLABa dokumentų aprašų informacijos (metaduomenų) prieiga tvarkymui priklauso nuo eLABa naudotojo vaidmens sistemoje, jo santykio su dokumentu ir dokumento būsenos dokumento apdorojimo procese;

17.3. eLABa tvarkytojai ir duomenų valdytojai gali tvarkyti tik savo institucijai priklausančius duomenis (dokumentų, klasifikatorių ir naudotojų duomenis), išskyrus sutartus bendro duomenų valdymo ar tvarkymo atvejus;

17.4. prieiga prie visateksčio elektroninio dokumento reglamentuojama teisiniais dokumentais, užtikrinančiais jo savininko intelektinės nuosavybės apsaugą;

17.5. duomenys į eLABa duomenų bazes gali būti įvesti, atnaujinami, naikinami, tik turint teisėtą pagrindą;

17.6. duomenų įvedimas, atnaujinimas, naikinimas registruojami elektroniniuose žurnaluose, nurodant eLABa naudotoją, darbo laiką, prisijungimo datą, atliktus veiksmus.

18. Informacinės sistemos eLABa naudotojų veiksmų registravimo tvarka:

18.1. elektroniniuose žurnaluose automatiškai registruojami eLABa naudotojo veiksmai su eLABa duomenimis;

18.2. eLABa taikomosios programinės įrangos administratorius gali peržiūrėti duomenų sukūrimo, redagavimo ar šalinimo veiksmus pagal atskirą objektą (pvz., dokumentą, klasifikatorių), naudotoją, instituciją, laiko intervalą.

19. Atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarka:

19.1. eLABa duomenų bazių ir archyvų valdymas organizuojamas, atsižvelgiant į eLABa nuostatų 40 punkto reikalavimus;

19.2. visa eLABa duomenų kopija daroma ne rečiau kaip kartą per savaitę, pokyčių (inkrementinė kopija) – ne rečiau kaip kartą per parą;

19.3. visos duomenų kopijos saugomos ne trumpiau kaip vieną mėnesį, pokyčių – ne trumpiau kaip vieną savaitę;

19.4. visos duomenų kopijos saugomos atskiroje patalpoje nuo pagrindinių eLABa tarnybinių stočių;

19.5. atsarginėse kopijose eLABa elektroninė informacija turi būti užšifruota;

19.6. duomenis atkurti iš atsarginės kopijos turi teisę eLABa sisteminis administratorius, prieš tai įsitikinęs, kad toks atkūrimas nesugadins esamų duomenų;

19.7. apie duomenų atkūrimą eLABa sisteminis administratorius privalo informuoti pagrindinį eLABa saugos įgaliotinį;

19.8. visiškas sistemos atkūrimas iš atsarginės kopijos turi užtrukti ne daugiau kaip 24 valandas.

20. eLABa elektroninės informacijos neteisėto duomenų kopijavimo, keitimo, naikinimo ar perdavimo nustatymo tvarka:

20.1. eLABa naudotojai, pastebėję neteisėto duomenų kopijavimo, keitimo, naikinimo, perdavimo ar kitus saugos dokumentų reikalavimų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai eLABa lokalaus tinklo ir darbo vietų administratoriui;

20.2. eLABa lokalaus tinklo ir darbo vietų administratorius jam prieinamomis programinėmis priemonėmis patikrina gautą pranešimą apie pažeidimą ir, faktui pasitvirtinus, jei to nepadarė kitas eLABa administratorius, registruoja incidentą pažeidimų žurnale adresu http://darbai.labt.lt/redmine bei imasi visų įmanomų prevencinių priemonių. Jei priemonės nepakankamos, informuoja eLABa sisteminį administratorių;

20.3. eLABa sisteminis administratorius išanalizuoja gautą informaciją, įvertina, ar nereikėtų papildomų prevencinių priemonių. Jei siūlomos papildomos priemonės, eLABa sisteminis administratorius informuoja pagrindinio eLABa tvarkytojo atsakingus asmenis ir eLABa saugos įgaliotinį.

21. Programinės ir techninės įrangos keitimo ir atnaujinimo tvarka:

21.1. eLABa programinės ir techninės įrangos atnaujinimui galioja pokyčių valdymo tvarka;

21.2. eLABa programinės ir techninės įrangos keitimo ir atnaujinimo tvarką su trečia šalimi, kuriai Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka perduotos informacinės sistemos ir (ar) jos infrastruktūros priežiūros funkcijos (toliau – paslaugų teikėjas), atsižvelgiant į konkretų atvejį, derina eLABa sisteminis ir taikomosios programinės įrangos administratoriai arba ji aprašoma paslaugų, susijusių su eLABa programinės ir techninės įrangos keitimu ir atnaujinimu, teikimo sutartyse ir sistemos priežiūros reglamentuose;

21.3. migravimą prie naujos operacinės sistemos versijos inicijuoja eLABa sisteminis administratorius, darbus suderinęs su eLABa administruojančios institucijos pagrindiniu administratoriumi ir taikomosios programinės įrangos administratoriumi;

21.4. apie visus darbus, kurie gali sutrikdyti eLABa sistemos veikimą, eLABa sisteminis arba taikomosios programinės įrangos administratoriai iš anksto privalo informuoti eLABa saugos įgaliotinį ir eLABa naudojančias institucijas.

22. eLABa pokyčių valdymo tvarka:

22.1. eLABa valdytojas užtikrina informacinės sistemos pokyčių (toliau – pokyčiai) valdymo planavimą, apimantį pokyčių identifikavimą, suskirstymą į kategorijas pagal pokyčio tipą

(administracinis, organizacinis ar techninis), įtakos vertinimą (svarbumas ir skubumas) ir pokyčių prioritetų nustatymo procesus;

22.2. eLABa duomenų valdymo įgaliotinis, vadovaudamasis eLABa plėtros planu, kitais valdytojo planavimo dokumentais:

22.2.1. vykdo eLABa pokyčių valdymo planavimą, apimantį pokyčių identifikavimą, suskirstymą į kategorijas pagal pokyčio tipą (administracinis, organizacinis ar techninis);

22.2.2. siūlo eLABa valdytojui pokyčio įtakos vertinimą (svarbumas ir skubumas) ir pokyčių prioritetą;

22.2.3. įgyvendina eLABa ar funkciškai savarankiškos jos sudedamosios dalies (toliau – posistemė) plėtrą;

22.2.4. tiesiogiai prižiūri, kaip kuriama ir tvarkoma eLABa sistema, jos posistemės ar funkciškai savarankiška sudedamoji dalis, diegiama programinė įranga, panaudojamos investicijos;

22.2.5. rengia eLABa biudžeto projektus;

22.3. pokyčiai identifikuojami, nustačius eLABa naudotojų, administratorių ir kitų vaidmenų poreikius, apibendrinus kylančias priežiūros problemas ir kitais gerosios praktikos įvardijamais atvejais;

22.4. pokyčius turi teisę inicijuoti eLABa duomenų valdymo įgaliotinis, pagrindinis eLABa saugos įgaliotinis ar eLABa taikomosios programinės įrangos administratorius, o įgyvendinti – eLABa sisteminis ar taikomosios programinės įrangos administratoriai pagal kompetenciją;

22.5. visi potencialūs pokyčiai registruojami pokyčių registre, įvertinus ir valdytojui patvirtinus įtakos vertinimą ir prioritetą;

22.6. kibernetiniam saugumui užtikrinti naudojamų priemonių diegimas ir šių priemonių parametrų keitimas laikomas pokyčiu ir atliekamas nustatyta pokyčių valdymo tvarka;

22.7. eLABa programinės įrangos pokyčiai atliekami, tik įvertinus pokyčio poreikį, pokyčio apimtį ir suderinus sistemos modernizavimo mastą;

22.8. eLABa sistemos funkcijų ir galimybių sąrankos aprašai turi būti nuolat atnaujinami ir rodyti esamą informacinės sistemos sąrankos būklę;

22.9. pokyčiai įgyvendinami eLABa valdytojo patvirtintu eiliškumu, atsižvelgiant į sutartą skubumą ar svarbumą;

22.10. visi diegiami pokyčiai, galintys sutrikdyti ar sustabdyti informacinės sistemos darbą, turi būti suderinti su eLABa duomenų valdymo ir saugos įgaliotiniais ir vykdomi, tik gavus jų raštišką pritarimą;

22.11. prieš atlikdamas eLABa pokyčius, kurių metu gali iškilti grėsmė duomenų ir eLABa konfidencialumui, vientisumui ar pasiekiamumui, eLABa taikomosios programinės įrangos administratorius privalo įsitikinti, kad planuojami eLABa pokyčiai išbandyti bandomojoje aplinkoje;

22.12. programinės įrangos testavimas atliekamas, naudojant atskirą tam skirtą testavimo aplinką, kurioje nėra konfidencialių ir asmens duomenų ir kuri atskirta nuo eksploatuojamos informacinės sistemos;

22.13. atlikus vykdomų eLABa pokyčių testavimą, eLABa taikomosios programinės įrangos administratorius gali pradėti įgyvendinti eLABa pokyčius, tik suderinęs su pagrindiniu eLABa administratoriumi;

22.14. planuodamas eLABa pokyčius, kurių metu galimi eLABa veikimo sutrikimai, eLABa taikomosios programinės įrangos administratorius privalo ne vėliau kaip prieš dvi darbo dienas iki eLABa pokyčių vykdymo pradžios elektroniniu paštu informuoti visus eLABa administratorius ir elektroniniu būdu interneto svetainėje www.elaba.lt informuoti eLABa naudotojus apie tokių darbų pradžią ir galimus eLABa veikimo sutrikimus.

23. eLABa sisteminių ir taikomosios programinės įrangos administratorių pareigoms atlikti skirtų nešiojamųjų kompiuterių naudojimo tvarka:

23.1. nešiojamieji kompiuteriai turi būti saugomi ir negali būti palikti be priežiūros viešose vietose;

23.2. visi nešiojamieji kompiuteriai turi būti apsaugoti saugiais slaptažodžiais, sudėtingumu atitinkančiais naudotojų administravimo taisyklių reikalavimus.

24. Elektroninio pašto naudojimo reikalavimai nustatyti Lietuvos mokslo ir studijų institucijų kompiuterių tinklo LITNET naudojimo taisyklėse, patvirtintose 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“.

IV SKYRIUS
REIKALAVIMAI, KELIAMI eLABa FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

25. Prireikus eLABa funkcionuoti reikalingoms paslaugoms praplėsti gali būti pritraukiami išorės tiekėjai, teisės aktų nustatyta tvarka sudarant su jais atitinkamas paslaugų teikimo sutartis.

26. Perkant paslaugas, darbus ar įrangą, susijusius su eLABa infrastruktūra, jos projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, pirkimo dokumentuose turi būti iš anksto nustatyta, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas užtikrina atitiktį Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, reikalavimams.

27. eLABa sisteminis administratorius atsako už programinių, techninių ir kitų prieigos prie eLABa resursų organizavimą, suteikimą ir panaikinimą techninės ir (ar) programinės paslaugos teikėjui.

28. eLABa sisteminis administratorius suteikia paslaugos teikėjui tik tokią prieigą prie eLABa resursų, kuri yra būtina norint atlikti arba vykdyti sutartyje nustatytus įsipareigojimus, kurie neprieštarauja įstatymų ir kitų teisės aktų reikalavimams.

29. Su paslaugų teikėju turi būti suderinta paslaugos teikimo tvarka, į kurią įtraukti prieigos reikalavimai bei jų suteikimo sąlygos.

30. Pasibaigus sutarties su paslaugos teikėjais galiojimo terminui ar atsiradus kitoms sutartyje ar saugos politiką įgyvendinančiuose dokumentuose įvardytoms sąlygoms, eLABa sisteminis administratorius nedelsdamas privalo panaikinti suteiktą prieigą.

31. Reikalavimai, keliami teikėjų patalpoms, įrangai, informacinės sistemos priežiūrai, duomenų perdavimui tinklais ir kitoms paslaugoms, nurodomi eLABa taikomosios programinės įrangos paslaugų teikimo sutartyse.

32. Teikėjų darbuotojams, atliekantiems administravimo funkcijas, taikomi visi atitinkamo lygio eLABa administratoriams saugos dokumentuose nustatyti reikalavimai.

_____

PATVIRTINTA
Lietuvos Respublikos švietimo ir mokslo ministro
2015 m. liepos 2 d. įsakymu Nr. V-710
(Lietuvos Respublikos švietimo, mokslo ir sporto ministro
2019 m. spalio 14 d. įsakymo Nr. V-1150
redakcija)

LIETUVOS AKADEMINĖS ELEKTRONINĖS BIBLIOTEKOS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos akademinės elektroninės bibliotekos informacinės sistemos veiklos tęstinumo valdymo plano tikslas – nustatyti Lietuvos akademinės elektroninės bibliotekos informacinės sistemos (toliau – eLABa) valdytojo, tvarkytojų, duomenų valdymo ir saugos įgaliotinių, administratorių, naudotojų ir kitų asmenų įgaliojimus ir veiksmus, siekiant apsisaugoti nuo elektroninių informacijos saugos ir kibernetinių incidentų (toliau – saugos incidentų) keliamų grėsmių arba likviduoti jų sukeltus padarinius eLABa duomenims bei eLABa techninės ir programinės įrangos funkcionavimui.

2. Lietuvos akademinės elektroninės bibliotekos informacinės sistemos veiklos tęstinumo valdymo planas (toliau – Planas) parengtas 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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, 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 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 kitais teisės aktais.

3. Planas įsigalioja nustačius vidutinio ar didesnio poveikio saugos incidentą, vadovaujantis Nacionalinio kibernetinių incidentų valdymo plane, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, nurodytais kriterijais.

4. Kibernetinius incidentus pavojingo incidento kategorijai turi teisę priskirti tik Nacionalinis kibernetinio saugumo centras.

5. Nustačius, kad incidentas priskirtinas nereikšmingų saugos incidentų kategorijai, šis sprendžiamas vadovaujantis Lietuvos akademinės elektroninės bibliotekos elektroninės informacijos ir kibernetinių saugos incidentų valdymo tvarka, numatyta Plano 2 priede.

6. Plane vartojamos sąvokos:

6.1. **Konsorciumo informacinių sistemų priežiūros darbo grupės** (toliau – KISP grupės) – funkcinės tarnybos, skirtos eLABa eksploatacijos techninei priežiūrai vykdyti. Į jų funkcijas įtraukiama eLABa techninės ir programinės įrangos darbo stebėsena, eksploatacinių problemų sprendimas, galimų sutrikimų prevencija, institucijų administratorių konsultavimas, bendrųjų eLABa klasifikatorių tvarkymas. eLABa eksploatacijai užtikrinti yra sukurti 2 techniniai centrai (po vieną Vilniaus universitete ir Kauno technologijų universitete), savo darbų sritį ir atsakomybę pasiskirstę eLABa posistemėmis;

6.2. kitos Plane vartojamos sąvokos suprantamos taip, kaip apibrėžtos Plano 2 punkte nurodytuose ir kituose saugų duomenų tvarkymą reglamentuojančiuose teisės aktuose.

7. Planas yra parengtas Vilniaus universiteto Informacinių technologijų paslaugų centrui (toliau – ITPC), esančiam Saulėtekio al. 9, Vilniuje, ir Kauno technologijos universiteto Informacinių technologijų departamentui (toliau – ITD), esančiam Studentų g. 48A, Kaune.

8. Šiuo Planu nustatomi šie informacinės sistemos veiklos tęstinumo tikslai:

8.1. per metus informacinės sistemos prieinamumas turi būti užtikrintas ne mažiau kaip 90 proc. laiko darbo metu darbo dienomis;

8.2. informacinės sistemos priežiūros ir atstatymo darbai vykdomi darbo dienomis darbo valandomis, išskyrus atvejus, kai informacinės sistemos valdytojas priima sprendimą dėl poreikio vykdyti veiklos atstatymo darbus neatidėliotinai.

9. Įvykus ekstremalioms situacijoms, šio Plano nuostatos galioja tiek, kiek neprieštarauja nuostatoms, reglamentuojamoms Lietuvos Respublikos civilinės saugos įstatyme ir ekstremaliųjų situacijų valdymo planuose.

10. Sprendimą dėl šio Plano aktyvavimo ir eLABa veiklos tęstinumą organizuojančios veiklos tęstinumo valdymo grupės (toliau – Valdymo grupė) sukvietimo priima eLABa duomenų valdymo įgaliotinis.

11. eLABa naudotojai, pastebėję eLABa veiklos sutrikimus, neveikiančias ar netinkamai veikiančias duomenų saugos užtikrinimo priemones, turi nedelsdami apie tai pranešti savo darbo vietos administratoriui arba darbo vietą administruojančiai tarnybai.

12. Darbo vietos administratorius, priėmęs pranešimą apie saugos incidentą, patikrina aplinkybes ir registruoja pranešimą saugos incidentų žurnale adresu http://darbai.labt.lt/redmine bei nedelsdamas telefonu praneša pagrindiniam eLABa administratoriui.

13. eLABa duomenų valdymo įgaliotinis:

13.1. įvertinęs saugos incidentą pagal vertinimo kriterijus priskiriant kategorijoms, numatytus Plano 3 priede, priima sprendimą dėl tolesnių veiksmų atkuriant veiklos tęstinumą;

13.2. organizuoja išteklius, reikalingus saugos incidentų padariniams šalinti;

13.3. informuoja valdytoją ir kitus tvarkytojus;

13.4. teikia informaciją suinteresuotiems asmenims ir žiniasklaidai;

13.5. vykdo kitas Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme numatytas pareigas ir funkcijas.

14. eLABa saugos įgaliotinis:

14.1. organizuoja vidutinio ir didesnio poveikio saugos incidentų tyrimą;

14.2. bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, saugos ir kibernetinius incidentus ir neteisėtas veiklas;

14.3. informuoja eLABa duomenų valdymo įgaliotinį apie incidento tyrimo eigą.

15. Plano nuostatų vykdymas privalomas eLABa valdytojui ir visiems eLABa tvarkytojams, visiems eLABa naudotojams, eLABa administratoriams, konsorciumo institucijų eLABa duomenų bei saugos įgaliotiniams.

16. eLABa saugos įgaliotinių, eLABa administratorių ir kitų eLABa naudotojų veiksmai bei funkcijos, įvykus eLABa saugos incidentui, nurodyti Lietuvos akademinės elektroninės bibliotekos informacinės sistemos veiklos atkūrimo detaliajame plane (1 priedas) ir Lietuvos

akademinės elektroninės bibliotekos saugos ir kibernetinių incidentų valdymo tvarkos apraše (2 priedas).

17. eLABa veiklai atkurti reikalingų finansinių ir kitokių išteklių poreikį, vadovaudamasis konsorciumo valdybos ir visuotinio susirinkimo nutarimais, nustato eLABa duomenų valdymo įgaliotinis, o reikiamus išteklius skiria eLABa valdytojas Lietuvos Respublikos švietimo, mokslo ir sporto ministerija ir eLABa vartotojai.

18. Laikoma, kad eLABa veikla yra atkurta, kai galima atlikti visus veiksmus Paieškos portale, Metaduomenų posistemėje, Komplektavimo posistemėje, Naudotojų administravimo posistemėje, El. objektų ilgalaikio saugojimo posistemėje, Dokumentų sutapties nustatymo posistemėje, Statistikos ir ataskaitų formavimo posistemėje ir Administravimo posistemėje.

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

PIRMASIS SKIRSNIS
eLABa VEIKLOS TĘSTINUMO VALDYMO GRUPĖ

19. eLABa veiklos tęstinumą organizuoja eLABa veiklos tęstinumo valdymo grupė (toliau – Valdymo grupė).

20. Valdymo grupės sudėtis:

20.1. Valdymo grupės vadovas – eLABa duomenų valdymo įgaliotinis;

20.2. Valdymo grupės nariai – KISP vadovai, eLABa saugos įgaliotinis ir kiti asmenys Valdymo grupės vadovo sprendimu.

21. Valdymo grupės vadovą jam negalint atvykti, atostogų metu ar išvykus pavaduoja pagal pareigas pavaduojantis asmuo.

22. Valdymo grupė atlieka šias funkcijas:

22.1. analizuoja didelio poveikio ir pavojingų eLABa saugos incidentų atsiradimo priežastis, pasekmes bei šių priežasčių šalinimo būdus;

22.2. analizuoja situaciją ir paprasta balsų dauguma priima sprendimus eLABa veiklos tęstinumo valdymo klausimais;

22.3. koordinuoja, kaip atliekami Plano 1 priede (Lietuvos akademinės bibliotekos informacinės sistemos veiklos atkūrimo detalusis planas) numatyti veiksmai;

22.4. prireikus, bendrauja su eLABa susijusių informacinių sistemų veiklos tęstinumo valdymo grupėmis;

22.5. prireikus, bendrauja su teisėsaugos ir kitomis institucijomis, konsorciumo nariais ir kitomis interesų grupėmis;

22.6. įvykus didelio poveikio ir pavojingiems eLABa saugos incidentams, įvertina finansinių ir kitų išteklių, reikalingų eLABa veiklai atkurti, poreikį ir kontroliuoja, kaip jie naudojami;

22.7. prireikus, organizuoja eLABa duomenų ir įrangos fizinę saugą;

22.8. koordinuoja logistiką (žmonių, daiktų, įrangos gabenimą ir jo organizavimą);

22.9. prireikus organizuoja prekių, paslaugų ir darbų, reikalingų eLABa veiklai atkurti, įsigijimą;

22.10. atlieka kitas Valdymo grupei pavestas funkcijas ir susijusius eLABa duomenų valdymo įgaliotinio nurodymus.

23. Valdymo grupė komunikuoja ne rečiau kaip kartą per 4 valandas didelio poveikio saugos incidento atveju ir ne rečiau kaip kartą per dvidešimt keturias valandas – vidutinio poveikio incidento atveju. Detalusis planas pateikiamas Plano 1 priede.

24. Su viešosios informacijos rengėjų ir skleidėjų atstovais bendrauja Valdymo grupės vadovas arba Konsorciumo valdybos pirmininkas.

25. Valdymo grupė organizuoja susirinkimą mažiausiai kartą per metus arba įvykus esminiams pokyčiams.

26. Kiti Valdymo grupės komunikavimo atvejai aprašomi Lietuvos akademinės elektroninės bibliotekos informacinės sistemos veiklos atkūrimo detaliajame plane (1 priedas).

27. Saugos incidento sprendimo metu eLABa Valdymo grupės nariai bendrauja mobiliojo ryšio telefonais, elektroniniu paštu ir pagal galimybes kitomis sutartomis ryšio priemonėmis. Visi Valdymo grupės nariai turi kitų narių mobiliojo ryšio telefonų numerius, elektroninio pašto adresus ir kitų sutartų ryšio priemonių identifikatorius (pagal galimybes).

ANTRASIS SKIRSNIS
eLABa VEIKLOS ATKŪRIMO GRUPĖ

28. Įvykus didelio poveikio ir pavojingiems incidentams eLABa paslaugas atkuria informacinės sistemos veiklos atkūrimo grupė (toliau – Atkūrimo grupė). Įvykus nereikšmingo ir vidutinio poveikio incidentams – eLABa paslaugas atkuria KISP grupė.

29. Atkūrimo grupės sudėtis:

29.1. Atkūrimo grupės vadovas – techninio centro, kuriame įvyko incidentas, KISP grupės vadovas;

29.2. Atkūrimo grupės vadovo pavaduotojas – kito techninio centro, nei tas, kuriame įvyko incidentas, vadovas;

29.3. Atkūrimo grupės nariai – eLABa pagrindinis, taikomosios programinės įrangos ir sisteminiai administratoriai, kiti Vilniaus universiteto ir Kauno technologijos universiteto techninių centrų vadovų paskirti darbuotojai.

30. Atkūrimo grupė atlieka šias funkcijas:

30.1. organizuoja eLABa tarnybinių stočių veikimo atkūrimą;

30.2. organizuoja eLABa kompiuterių tinklo veikimo atkūrimą;

30.3. organizuoja eLABa elektroninės informacijos atkūrimą;

30.4. organizuoja tinkamą eLABa taikomųjų programų veikimo atkūrimą;

30.5. organizuoja darbo vietų kompiuterių veikimo ir prijungimo prie tinklo atkūrimą;

30.6. atlieka kitas Atkūrimo grupei pavestas funkcijas.

31. Techninių centrų Atkūrimo grupių vardinę sudėtį ir kontaktinę informaciją tvirtina techninių centrų vadovai.

32. Atkūrimo grupė renkasi techninio centro, kuriame įvyko saugos incidentas, vadovo, KISP grupės vadovo, duomenų valdymo įgaliotinio arba eLABa saugos įgaliotinio sprendimu.

33. Apie atkūrimo eigą Valdymo grupę informuoja Atkūrimo grupės vadovas arba pavaduojantis asmuo. Informuojama arba įvykdžius sutartą veiklą, arba jei nesutarta kitaip – toliau nustatytais terminais:

33.1. apie didelio poveikio incidentų valdymo būklę – ne vėliau kaip per keturias valandas nuo jų nustatymo ir ne rečiau kaip kas keturias valandas pateikiant atnaujintą informaciją, iki incidentas suvaldomas ar pasibaigia;

33.2. apie vidutinio poveikio incidentų valdymo būklę – ne vėliau kaip per dvidešimt keturias valandas nuo jų nustatymo ir ne rečiau kaip kas dvidešimt keturias valandas pateikiant atnaujintą informaciją, iki incidentas suvaldomas ar pasibaigia;

33.3. apie didelio ar vidutinio poveikio incidentų suvaldymą ar pasibaigimą – ne vėliau kaip per keturias valandas nuo jų suvaldymo ar pasibaigimo.

34. Papildomi Valdymo ir Atkūrimo grupių komunikavimo atvejai aprašomi Plano 1 priede.

35. Apie atkūrimo eigą Valdymo grupę informuoja Atkūrimo grupės vadovas arba pavaduojantis asmuo.

36. Kiti Atkūrimo grupės komunikavimo atvejai aprašomi Plano 1 priede (Lietuvos akademinės bibliotekos informacinės sistemos veiklos atkūrimo detalusis planas).

37. Saugos incidento metu eLABa Atkūrimo grupės nariai bendrauja mobiliojo ryšio telefonais, elektroniniu paštu ir pagal galimybes kitomis sutartomis ryšio priemonėmis. Visi Atkūrimo grupės nariai turi kitų narių mobiliojo ryšio telefonų numerius, elektroninio pašto adresus ir kitų sutartų ryšio priemonių identifikatorius (pagal galimybes). Prireikus Valdymo ir Atkūrimo grupės rengia bendrus susirinkimus.

TREČIASIS SKIRSNIS
REIKALAVIMAI, KELIAMI ATSARGINĖMS PATALPOMS, NAUDOJAMOMS INFORMACINĖS SISTEMOS VEIKLAI ATKURTI, ĮVYKUS ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTUI, ATSARGINIŲ PATALPŲ ADRESAI IR BŪDAI, KAIP IKI JŲ NUVYKTI

38. Šalinant saugos incidento padarinius, eLABa veiklai atkurti prireikus gali būti naudojamos atsarginės patalpos.

39. Atsarginės patalpos atitinka eLABa saugaus elektroninės informacijos tvarkymo taisyklėse nurodytus reikalavimus.

40. Atsarginėms patalpoms, naudojamoms eLABa veiklai atkurti incidento šalinimo metu, keliami šie reikalavimai:

40.1. patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų;

40.2. patalpose turi būti įrengta langų ir durų fizinė apsauga;

40.3. patalpos privalo atitikti priešgaisrinės saugos reikalavimus, jose turi būti gaisro gesinimo priemonės;

40.4. ryšių kabeliai turi būti apsaugoti nuo neteisėto prisijungimo prie jų ir pažeidimo;

40.5. privalo būti įgyvendintos įrangos gamintojo nustatytos techninės įrangos darbo sąlygos;

40.6. patalpose turi būti patikimas elektros energijos tiekimas per nenutrūkstamo maitinimo šaltinius;

40.7. patalpose būtina duomenų perdavimo tinklo ir interneto ryšio prieiga;

40.8. atsarginės patalpos turi atitikti ir kitus eLABa saugaus elektroninės informacijos tvarkymo taisyklėse ir pagrindinio tvarkytojo duomenų centro reglamente bei *Tier* II lygio duomenų centrams taikomus nurodytus reikalavimus.

41. Atsarginių patalpų adresai:

41.1. Vilniaus universiteto ITPC pastatui, esančiam Saulėtekio al. 9, Vilniuje, atsarginės patalpos yra numatytos Kauno technologijos universiteto ITD pastate, esančiame Studentų g. 48A, Kaune;

41.2. Kauno technologijos universiteto ITD pastatui, esančiame Studentų g. 48A, Kaune, atsarginės patalpos yra numatytos Vilniaus universiteto ITPC pastate, esančiam Saulėtekio al. 9, Vilniuje.

42. Nuvykimo į atsargines patalpas organizaciniai principai ir būdai:

42.1. Valdymo grupės užsakymus darbuotojams ir technikai pervežti:

42.1.1. iš Vilniaus universiteto ITPC patalpų į atsargines organizuoja Vilniaus universiteto Turto valdymo ir paslaugų centro Paslaugų skyrius;

42.1.2. iš Kauno technologijos universiteto ITD patalpų į atsargines organizuoja Kauno technologijos universiteto Paslaugų departamento Transporto grupė.

42.2. Veiklos tęstinumo Valdymo ir Atkūrimo grupių nariai, gavę nurodymą vykti į atsargines patalpas, vyksta:

42.3. iš Vilniaus universiteto ITPC į Kauno technologijos universiteto ITD Vilniaus universiteto organizuojamu transportu;

42.4. iš Kauno technologijos universiteto ITD į Vilniaus universiteto ITPC Kauno technologijos universiteto organizuojamu transportu;

42.5. esant būtinybei, darbuotojai atvyksta savo arba viešuoju transportu:

42.6. vykstant iš Vilniaus universiteto ITPC į Kauno technologijos universiteto ITD, Vilniaus universiteto rektoriaus numatyta tvarka apmokamos būtinosios transporto išlaidos;

42.7. vykstant iš Kauno technologijos universiteto ITD į Vilniaus universiteto ITPC, Kauno technologijos universiteto rektoriaus numatyta tvarka apmokamos būtinosios transporto išlaidos.

KETVIRTASIS SKIRSNIS
KIBERNETINIŲ INCIDENTŲ TYRIMAS IR ANALIZĖ

43. eLABa kibernetinių incidentų, kuriuos sprendžiant buvo priimtas sprendimas aktyvinti Planą, tyrimas ir analizė, tiek, kiek to nereglamentuoja Nacionalinis kibernetinių incidentų valdymo planas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, atliekami Plano 2 priede nustatyta tvarka.

44. eLABa tvarkytojas, kurio ryšių ir informacinėje sistemoje tirtas kibernetinis incidentas, išanalizavęs ir įvertinęs visą informaciją, susijusią su eLABa kibernetiniu incidentu, atliktus veiksmus ir panaudotas priemones:

44.1. ne vėliau kaip per trisdešimt darbo dienų po eLABa kibernetinio incidento suvaldymo ar pasibaigimo pateikia eLABa kibernetinio incidento analizės rezultatus Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos ir kibernetinio saugumo informaciniame tinkle paskelbia susistemintą ir aktualią neįslaptintą informaciją apie eLABa kibernetinio incidento nustatymą ir suvaldymą;

44.2. imasi priemonių, kad būtų pašalintas ryšių ir informacinės sistemos pažeidžiamumas;

44.3. įvertina ryšių ir informacinės sistemos riziką ir atitiktį Vyriausybės nustatytiems organizaciniams ir techniniams eLABa kibernetinio saugumo reikalavimams;

44.4. nustačius teisinio reglamentavimo spragas, pakeičia eLABa kibernetinio saugumo teisės aktus ir (ar) inicijuoja kitų institucijų priimtų teisės aktų pakeitimus.

45. eLABa tvarkytojai Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos pateikia kibernetinio incidento tyrimo ataskaitą apie:

45.1. didelio poveikio kibernetinių incidentų valdymo būklę – ne vėliau kaip per keturias valandas nuo jų nustatymo ir ne rečiau kaip kas keturias valandas atnaujintą informaciją, iki kibernetinis incidentas suvaldomas ar pasibaigia;

45.2. vidutinio poveikio kibernetinių incidentų valdymo būklę – ne vėliau kaip per dvidešimt keturias valandas nuo jų nustatymo ir ne rečiau kaip kas dvidešimt keturias valandas atnaujintą informaciją, iki kibernetinis incidentas suvaldomas ar pasibaigia;

45.3. didelio ar vidutinio poveikio kibernetinių incidentų suvaldymą ar pasibaigimą – ne vėliau kaip per keturias valandas nuo jų suvaldymo ar pasibaigimo.

46. Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos teikiant didelio ar vidutinio poveikio kibernetinio incidento tyrimo ataskaitą nurodoma eLABa tvarkytojui žinoma informacija:

46.1. kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal Nacionaliniame kibernetinių incidentų valdymo plane, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“, nustatytus kriterijus;

46.2. ryšių ir informacinės sistemos, kurioje nustatytas kibernetinis incidentas, tipas (informacinė sistema);

46.3. kibernetinio incidento veikimo trukmė;

46.4. kibernetinio incidento šaltinis;

46.5. kibernetinio incidento požymiai;
46.6. kibernetinio incidento veikimo metodas;
46.7. galimos ir (ar) nustatytos kibernetinio incidento pasekmės;
46.8. kibernetinio incidento poveikio pasireiškimo (galimo išplitimo) mastas;
46.9. kibernetinio incidento būsena (aktyvus, pasyvus);
46.10. priemonės, kuriomis kibernetinis incidentas nustatytas;
46.11. galimos ir (ar) taikomos kibernetinio incidento valdymo priemonės;
46.12. tikslus laikas, kada bus teikiama pakartotinė kibernetinio incidento tyrimo ataskaita.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

47. Plano ir susijusių dokumentų saugojimo ir atnaujinimo nuostatos:

47.1. skaitmeninės Plano, duomenų centro projektinės dokumentacijos ir įsigytos įrangos pirkimo sutarčių kopijos saugomos Vilniaus universiteto ir Kauno technologijos universiteto dokumentų valdymo sistemose, o taip pat elektroninėje laikmenoje kartu su Planu ir atsarginėmis kopijomis;

47.2. informacinės sistemos veiklai užtikrinti reikiamos informacinių technologijų įrangos ir jos parametrų konfigūracijos sąrašai yra administruojami pagrindinio eLABa administratoriaus, saugomi elektroninėse laikmenose ir konfigūracijos valdymo sistemos priemonėmis bei yra nuolat atnaujinami pasikeitimo atveju;

47.3. informacinės sistemos tvarkymui naudojamų patalpų brėžiniai, šiose patalpose esančios elektros įvado, kondicionavimo ir gesinimo įrangos išdėstymo, taip pat archyvinių įrenginių bei kamieninio kompiuterių tinklo fizinio ir loginio sujungimo schemos saugomos kartu su duomenų centro projektine dokumentacija tam skirtoje eLABa tvarkytojo patalpoje;

47.4. duomenų saugyklų infrastruktūros schemos, tarnybinių stočių paskirties ir aplikacijų diegimo schema, kompiuterių tinklo schema, kompiuterinės technikos ir sisteminės programinės įrangos sąrašai ir techniniai parametrai pateikti eLABa techniniame aprašyme (specifikacijoje) ir diegimo dokumentacijoje;

47.5. eLABa programinės įrangos laikmenos, reikalingos atkūrimui, saugomos eLABa tvarkytojo taikomosios programinės įrangos administratorių, programinės įrangos kodui ir jo versionavimui skirtame serveryje, o eLABa duomenų atsarginės kopijos – duomenų saugyklose;

47.6. Valdymo ir Atkūrimo grupių narių sąrašas su kontaktiniais duomenimis, leidžiančiais pasiekti šiuos asmenis bet kuriuo metu (mobiliųjų arba namų telefonų numeriai ir gyvenamųjų vietų adresai), pateikiami šių grupių nariams elektroninėje laikmenoje ir saugomi kartu su Planu;

47.7. Kontaktinius Valdymo ir Atkūrimo grupių darbuotojų duomenis atnaujina eLABa tvarkytojo IT pagalbos skyrius;

47.8. pagrindinę Plano kopiją tvarko ir saugo pagrindinis eLABa informacinės sistemos administratorius, atsargines elektronines kopijas saugo KISP grupės vadovai, pagrindinio eLABa tvarkytojo IT pagalbos vadovas ir eLABa saugos įgaliotinis;

47.9. Planas ir susiję dokumentai registruojami informacinės sistemos dokumentacijai skirtoje byloje, atnaujinamoje pasikeistus dokumentacijos plano bylų nomenklatūrai, dokumentų saugojimo vietai ar atsakingiems asmenims.

48. Nesant kurio nors eLABa sistemos administratoriaus, eLABa veiklą atkuria pavaduojantys administratoriai ir specialistai, išmanantys, kaip nustatyti:

48.1. eLABa tarnybinių stočių sąranką;
48.2. eLABa operacinių sistemų sąranką;
48.3. eLABa kompiuterių tinklo sąranką;
48.4. eLABa taikomosios programinės įrangos sąranką.

49. Reikiamos kompetencijos ir žinių lygio aprašus bei darbo instrukcijas rengia, nuolat atnaujina ir saugo eLABa sisteminiai administratoriai.

50. Valdymo ir Atkūrimo grupių narių sąrašas su kontaktiniais duomenimis, leidžiančiais pasiekti šiuos asmenis bet kuriuo metu (mobiliųjų arba namų telefonų numeriai ir gyvenamųjų vietų adresai), pateikiami šių grupių nariams ir saugomi kartu su Planu.

51. Asmenys, susipažindami su Plano 49 punkte nurodytais dokumentais, neturi teisės jų atskleisti ir privalo neaptarinėti su nesusijusiais asmenimis.

52. Planas viešai neskelbiamas. Su šiuo Planu dokumentų valdymo sistemos priemonėmis supažindinami eLABa administratoriai ir vidiniai eLABa naudotojai, tiesiogiai atsakingi už šio Plano vykdymą. Atsakingų asmenų supažindinimą organizuoja informacinės sistemos eLABa saugos įgaliotinis.

IV SKYRIUS
PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

53. Plano veiksmingumas išbandomas ne rečiau kaip kartą per metus.

54. Pagal Valdymo ir Atkūrimo grupių sumodeliuotą scenarijų simuliuojant sutarto poveikio saugos incidentą išbandymo metu aptariamas Plano veiksmingumas.

55. Plano išbandymo scenarijų, duomenų valdymo įgaliotinio nurodymu, rengia Atkūrimo grupė.

56. Plano išbandymo scenarijus suderinamas su Valdymo grupe ir kitais suinteresuotais asmenimis pagal poreikį.

57. Plano išbandymo scenarijų tvirtina eLABa duomenų valdymo įgaliotinis.

58. Plano išbandymą inicijuoja ir skelbia Valdymo grupės vadovas.

59. Plano veiksmingumo išbandyme dalyvauja Atkūrimo grupės nariai, eLABa saugos įgaliotinis ir Valdymo grupės nariai pagal poreikį.

60. Nustatytą dieną imituojamos nenumatytos situacijos, kurių metu atsakingi eLABa sisteminiai ir taikomosios programinės įrangos administratoriai atlieka būtinus tokiose situacijose veiksmus.

61. Prireikus, į Plano veiksmingumo išbandymą gali būti pakviesti kiti darbuotojai, rangovų arba kitų organizacijų atstovai.

62. Plano veiksmingumo išbandymo metu Atkūrimo grupė išanalizuoja galimą (sumodeliuotą) saugos incidentą, parengia Plano veiksmingumo išbandymo ataskaitą (Plano 5 priedas).

63. Įvykus Plano išbandymui, Valdymo grupė numato papildomas prevencines ir rizikos valdymo priemones.

64. Visa informacija, gauta Plano veiksmingumo išbandymo metu, perduodama eLABa saugos įgaliotiniui ir eLABa duomenų valdymo įgaliotiniui.

65. Už Plano veiksmingumo išbandymo metu pastebėtų trūkumų šalinimą atsakingas Atkūrimo grupės vadovas ir eLABa sistemos administratorius.

66. Išbandžius Planą, atsižvelgiant į gautus rezultatus ir (arba) įvertinus rizikos veiksnius, atliekamas Plano atnaujinimas.

67. Atsižvelgiant į gautus Plano veiksmingumo išbandymo rezultatus, Planas atitinkamai tikslinamas.

68. Plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami, vadovaujantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

_____

PATVIRTINTA
Lietuvos Respublikos švietimo ir mokslo ministro
2015 m. liepos 2 d. įsakymu Nr. V-710
(Lietuvos Respublikos švietimo, mokslo ir sporto ministro
2019 m. spalio 14 d. įsakymo Nr. V-1150
redakcija)

LIETUVOS AKADEMINĖS ELEKTRONINĖS BIBLIOTEKOS INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos akademinės elektroninės bibliotekos informacinės sistemos naudotojų administravimo taisyklės (toliau – Naudotojų administravimo taisyklės) reglamentuoja Lietuvos akademinės elektroninės bibliotekos informacinės sistemos (toliau – eLABa) 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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. nutarimu Nr. 1209 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl nacionalinės kibernetinio saugumo strategijos patvirtinimo“ pakeitimo“, 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 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 – Duomenų saugos nuostatai), 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. elektroninių tezių ir disertacijų duomenų bazė (toliau – ETD) – duomenų bazė, skirta kaupti Lietuvos mokslo ir studijų institucijų tvirtinamus studijų baigiamuosius darbus, daktaro disertacijas ir jų santraukas ir tvarkyti jų metaduomenis;

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

5.4. elektroninių dokumentų sutapties nustatymo sistema (toliau - ESAS) – eLABa posistemė, skirta dokumentų panašumui nustatyti ir plagiato kontrolės funkcijai vykdyti;

5.5. kitos Naudotojų administravimo taisyklėse vartojamos sąvokos suprantamos taip, kaip apibrėžtos Lietuvos akademinės elektroninės bibliotekos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse ir Naudotojų administravimo taisyklių 4 punkte nurodytuose teisės aktuose.

II SKYRIUS
eLABa NAUDOTOJŲ IR ADMINISTRATORIŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

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

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

8. Baigę darbą, eLABa naudotojai turi atsijungti nuo eLABa ir uždaryti programinę įrangą.

9. eLABa naudotojai privalo:

9.1. užtikrinti jų eLABa tvarkomų duomenų konfidencialumą bei vientisumą;

9.2. savo veiksmais netrikdyti eLABa duomenų prieinamumo;

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

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

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

9.6. atsakingai rinkti, vesti, naikinti ir kitaip tvarkyti duomenis;

9.7. taikyti saugos politiką įgyvendinančiuose dokumentuose numatytas elektroninės informacijos tvarkymo programines priemones;

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

10. eLABa naudotojai skirstomi į autorius, darbo vadovus, valdytojo ir tvarkytojų atsakingus asmenis, bibliotekininkus, padalinių registratorius, registratorius.

11. Autoriams suteikiama teisė:

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

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

11.3. formuoti savo duomenų ataskaitas.

12. Darbo vadovams suteikiama teisė:

12.1. peržiūrėti, redaguoti, tvirtinti ETD dokumentus;

12.2. peržiūrėti, redaguoti jiems priskirtų ETD dokumentų tikrinimo ESAS rezultatus.

13. Tvarkytojų atsakingiems asmenims suteikiama teisė peržiūrėti jiems priskirtus ETD dokumentus bei dokumentų tikrinimo ESAS rezultatus.

14. Bibliotekininkams suteikiama teisė:

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

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

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

14.4. formuoti savo institucijos ataskaitas.

15. Institucijų padalinių registratoriams suteikiama teisė:

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

15.2. formuoti savo padalinio ataskaitas.

16. Institucijų registratoriams suteikiama teisė:

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

16.2. įvesti, redaguoti ir tvirtinti specifinius savo institucijos metaduomenis, savo institucijos autorių dokumentus;

16.3. formuoti savo institucijos ataskaitas.

17. eLABa naudotojams negali būti suteikiamos eLABa administratoriaus teisės.

18. eLABa administratorių prieigos prie informacinių sistemų lygiai:

18.1. eLABa administratoriaus funkcijos turi būti atliekamos naudojant atskirą tam skirtą paskyrą, kuri negali būti naudojama kasdienėms eLABa naudotojo funkcijoms atlikti;

18.2. jeigu tas pats darbuotojas yra ir eLABa naudotojas, ir eLABa administratorius, jam sukuriamos dvi atskiros paskyros su atitinkamomis prieigos teisėmis;

18.3. eLABa administratoriui turi būti apribotos prieigos teisės pagal jo atliekamas eLABa administravimo funkcijas;

18.4. pagrindinio eLABa tvarkytojo paskirtas eLABa naudotojų teisių administratorius administruoja visų eLAba naudotojų prieigos teises prie eLAba, išskyrus eLABa Tvarkytojų paskirtų eLABa naudotojų teisių administratorių administruojamus naudotojus;

18.5. kitų eLABa administratorių funkcijos ir prieigos lygiai įvardyti Duomenų saugos nuostatuose, pareigybių aprašymuose;

18.6. eLABa Tvarkytojų paskirti eLABa naudotojų teisių administratoriai administruoja savo institucijos eLABa naudotojus.

III SKYRIUS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO eLABa NAUDOTOJAMS KONTROLĖS TVARKA

19. eLABa naudotojų registravimo ir išregistravimo tvarka:

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

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

19.3. eLABa duomenų valdytojas, 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.

20. Priemonės eLABa naudotojų tapatybei nustatyti:

20.1. eLABa naudotojui jungiantis prie sistemos, jo tapatybė nustatoma pagal unikalų eLABa naudotojo identifikatorių, patvirtinamą asmeniniu slaptažodžiu;

20.2. identifikatoriumi negali būti asmens kodas.

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

21.1. slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių;

21.2. slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pavyzdžiui, gimimo data, šeimos narių vardai ir panašiai).

21.3. draudžiama slaptažodžius atskleisti kitiems asmenims;

21.4. eLABa dalys, patvirtinančios eLABa naudotojo tapatumą, turi drausti automatiškai išsaugoti slaptažodžius;

21.5. turi būti nustatytas didžiausias leistinas eLABa naudotojo mėginimų įvesti teisingą slaptažodį skaičius (ne daugiau kaip 5 kartai). Iš eilės neteisingai įvedus slaptažodį tiek kartų, kiek nustatyta, eLABa naudotojo paskyra turi užsirakinti ir neleisti eLABa naudotojui patvirtinti tapatybės kibernetinio saugumo reikalavimų tvarkos apraše nustatytą laiką – ne trumpiau kaip 15 minučių;

21.6. slaptažodžiai negali būti saugomi ar perduodami atviru tekstu. Tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jeigu eLABa naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra techninių galimybių eLABa naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu;

21.7. papildomi eLABa naudotojo slaptažodžių reikalavimai:

21.7.1. slaptažodis turi būti keičiamas ne rečiau kaip kas 3 mėnesius;

21.7.2. slaptažodį turi sudaryti ne mažiau kaip 8 simboliai;

21.7.3. keičiant slaptažodį, eLABa neturi leisti sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių;

21.7.4. pirmąkart jungiantis prie eLABa, turi būti reikalaujama, kad eLABa naudotojas pakeistų slaptažodį;

21.8. papildomi eLABa administratorių slaptažodžių reikalavimai:

21.8.1. slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius;

21.8.2. slaptažodį turi sudaryti ne mažiau kaip 12 simbolių;

21.8.3. keičiant slaptažodį, taikomoji programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių 3 paskutinių slaptažodžių.

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

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

22.2. eLABa naudotojų teisių administratorius, iš pagrindinio eLABa tvarkytojo gavęs rašytinį prašymą apriboti eLABa naudotojo prieigos teises, nedelsiant sustabdo nurodyto eLABa naudotojo prieigą prie eLABa;

22.3. eLABa naudotojams prieigos prie eLABa teisės nutraukiamos automatiškai, sistemai nustačius eLABa 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);

22.4. eLABa administratorius, gavęs eLABa tvarkytojo įgalioto darbuotojo nurodymą, gali sustabdyti eLABa naudotojo prieigą prie sistemos;

22.5. jei kyla grėsmė eLABa duomenų saugumui, pagrindinio eLABa tvarkytojo administratorius turi teisę sustabdyti eLABa naudotojo prieigą, informuodamas apie tai įgaliotą institucijos darbuotoją;

22.6. eLABa administratoriui ar naudotojui teisė dirbti su konkrečia elektronine informacija yra ribojama, sustabdant visas eLABa administratoriui ar naudotojui suteiktas prieigos prie eLABa teises, kai eLABa administratorius nesijungė prie sistemos daugiau nei du mėnesius, o eLABa naudotojas nesijungė prie sistemos daugiau nei tris mėnesius, vyksta eLABa administratoriaus ar naudotojo veiklos tyrimas ar jis nušalinamas nuo darbo (pareigų), neatitinka kituose teisės aktuose nustatytų eLABa naudotojo ar eLABa administratoriaus kvalifikacinių reikalavimų, taip pat pasibaigia jo darbo (tarnybos) santykiai, jis praranda patikimumą, eLABa administratorius ar naudotojas neteikia informacijos apie saugą užtikrinančių sistemos komponentų būklę ar atsisako vykdyti eLABa saugos įgaliotinio nurodymus ir pavedimus;

22.7. 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.

23. Leistini nuotolinio prisijungimo būdai:

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

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

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

_____

Lietuvos akademinės elektroninės
bibliotekos informacinės sistemos veiklos
tęstinumo
valdymo plano
1 priedas

LIETUVOS AKADEMINĖS ELEKTRONINĖS BIBLIOTEKOS INFORMACINĖS SISTEMOS VEIKLOS ATKŪRIMO DETALUSIS PLANAS

Eil. Nr.	Grėsmė	Pirminiai veiksmai	Pasekmių likvidavimo veiksmai	Atsakingi vykdytojai
1.	Nukentėjo patalpos viename iš techninių centrų (dėl gaisro, gamtos reiškinių ir kt. pavojaus)	1.1. Saugos incidento padarinių įvertinimas, priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas ir įgyvendinimas	1.1.1. Saugos incidento metu padarytos žalos įvertinimas	Valdymo grupė, Atkūrimo grupė
			1.1.2. Jei yra nukentėjusiųjų, pirmosios pagalbos suteikimas nukentėjusiems darbuotojams, kiti veiksmai, kaip numatyta darbų saugos instrukcijoje	Techninio centro darbuotojas, atsakingas už darbuotojų saugą ir sveikatą
			1.1.3. Priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas, darbuotojų informavimas	Valdymo grupė, Atkūrimo grupė
			1.1.4. Padarytą žalą likviduojančių darbuotojų instruktavimas	Techninio centro darbuotojas, atsakingas už darbuotojų saugą ir sveikatą, Atkūrimo grupės vadovas, techninio centro eLABa sisteminis administratorius
			1.1.5. Paslaugų negaunančių padalinių ir organizacijų informavimas	Valdymo grupė, Atkūrimo grupė

Eil. Nr.	Grėsmė	Pirminiai veiksmai	Pasekmių likvidavimo veiksmai	Atsakingi vykdytojai
			1.1.6. Saugos incidento metu padarytos žalos likvidavimas	Atkūrimo grupė, techninio centro darbuotojas, atsakingas už darbuotojų saugą ir sveikatą
		1.2. Galimybių dirbti nuotoliniu būdu ir pavaduojančių darbuotojų nuotolinėje vietoje instruktavimas	1.2.1. Darbuotojų, galinčių pavaduoti iš kito techninio centro arba dirbti nuotoliniu būdu iš kitų patalpų informavimas.	Valdymo grupė, Atkūrimo grupė
			1.2.2. Darbuotojų, galinčių atlikti pareigas nuotoliniu būdu, informavimas.	Valdymo grupė, Atkūrimo grupė
		1.3. Veiklos funkcijų atkūrimo vertinimas	1.3.1. Visiško funkcijų atkūrimo vertinimas, susijusių padalinių ir organizacijų informavimas	Valdymo grupė, Atkūrimo grupė
2.	Gaisras	2.1. Priešgaisrinės gelbėjimo tarnybos informavimas, darbuotojų evakavimas, civilinės saugos tarnybos informavimas	2.1.1. Įvykio vietos lokalizavimas	Techninio centro darbuotojas, atsakingas už darbuotojų saugą ir sveikatą
			2.1.2. Galimybių evakuoti darbuotojus nagrinėjimas	Techninio centro darbuotojas, atsakingas už darbuotojų saugą ir sveikatą, Valdymo grupė
			2.1.3. Darbuotojų informavimas apie evakuaciją	Techninio centro darbuotojas, atsakingas už darbuotojų saugą ir sveikatą
			2.1.4. Darbuotojų informavimas apie saugų darbą pavojaus zonoje	Valdymo grupė, Atkūrimo grupė, techninio centro darbuotojas, atsakingas už darbuotojų saugą ir sveikatą
			2.1.5. Saugos incidento metu padarytos žalos įvertinimas	Valdymo grupė, Atkūrimo grupė
			2.1.6. Padarytą žalą likviduojančių darbuotojų instruktavimas	Atkūrimo grupės vadovas, sisteminis administratorius

Eil. Nr.	Grėsmė	Pirminiai veiksmai	Pasekmių likvidavimo veiksmai	Atsakingi vykdytojai
			2.1.6. Paslaugų negaunančių padalinių ir organizacijų informavimas	Valdymo grupė, Atkūrimo grupė
			2.1.8. Saugos incidento metu padarytos žalos likvidavimas	Atkūrimo grupė
		2.2. Papildomą riziką keliančių faktorių (elektra, vanduo) pavojaus zonoje išjungimas	2.2.1. Gaisro gesinimas ankstyvoje stadijoje, jei yra rekomendacija dirbti pavojaus zonoje	Techninio centro darbuotojas, atsakingas už darbuotojų saugą ir sveikatą, Atkūrimo grupė, išorinė tarnyba
		2.3. Sutrikimų pašalinimas	2.3.1. Saugos incidento metu padarytos žalos likvidavimas	Atkūrimo grupė
		2.4. Veiklos funkcijų atkūrimo vertinimas	2.4.1. Visiško funkcijų atkūrimo vertinimas, susijusių padalinių ir organizacijų informavimas	Valdymo grupė, Atkūrimo grupė
3.	Elektros energijos tiekimo sutrikimai	3.1. Elektros energijos tiekimo sutrikimo priežasčių nustatymas	3.1.1. Rekomendacijų iš elektros energijos tiekimo tarnybos gavimas	Techninio centro darbuotojas, atsakingas už darbuotojų saugą ir sveikatą
			3.1.2. Padarytos žalos įvertinimas	Atkūrimo grupės vadovas, infrastruktūros grupės specialistas
			3.1.3. Paslaugų negaunančių padalinių ir organizacijų informavimas	Valdymo grupė, Atkūrimo grupė
		3.2. Darbuotojų instruktavimas	3.2.1. Žalą likviduojančių darbuotojų instruktavimas	Techninio centro darbuotojas, atsakingas už darbuotojų saugą ir sveikatą, Atkūrimo grupės vadovas
		3.3. Sutrikimų pašalinimas	3.3.1. Tarnybinių stočių, kitos techninės įrangos maitinimo elektros energijos išjungimas	Techninio centro darbuotojas, atsakingas už elektros tiekimo sistemų priežiūrą

Eil. Nr.	Grėsmė	Pirminiai veiksmai	Pasekmių likvidavimo veiksmai	Atsakingi vykdytojai
			3.3.2. Kreipimasis į elektros energijos tiekimo tarnybą dėl pavojaus trukmės ir sutrikimo pašalinimo galimybių	Techninio centro darbuotojas, atsakingas už elektros tiekimo sistemų priežiūrą
			3.3.3. Padarytos žalos likvidavimas	Išorinė elektros tinklo priežiūros tarnyba, eLABa sisteminis administratorius, atsakingas už elektros tiekimo sistemų priežiūrą
		3.4. Veiklos funkcijų atkūrimo vertinimas	3.4.1. Visiško funkcijų atkūrimo vertinimas, susijusių padalinių ir organizacijų informavimas	Valdymo grupė, Atkūrimo grupė
4.	Oro kondicionavimo sistemos sutrikimai	4.1. Oro kondicionavimo sistemos sutrikimo priežasčių nustatymas	4.1.1. Priežiūros tarnybos informavimas, rekomendacijų iš priežiūros tarnybos gavimas	eLABa sisteminis administratorius, techninio centro darbuotojas, atsakingas už oro kondicionavimo sistemos priežiūrą
			4.1.2. Padarytos žalos įvertinimas	eLABa sisteminis administratorius, techninio centro darbuotojas, atsakingas už oro kondicionavimo sistemos priežiūrą
		4.2. Darbuotojų instruktavimas	4.2.1. Žalą likviduojančių darbuotojų instruktavimas	Valdymo grupė, Atkūrimo grupė
			4.2.2. Darbuotojų informavimas, jei darbas esamose patalpose negali būti tęsiamas, darbo kitose patalpose ir nuotoliniu būdu organizavimas	Valdymo grupė, Atkūrimo grupė

Eil. Nr.	Grėsmė	Pirminiai veiksmai	Pasekmių likvidavimo veiksmai	Atsakingi vykdytojai
		4.3. Sutrikimų pašalinimas	4.3.1. Tikslios kontrolės oro kondicionierių / šaldymo mašinos pakartotinas įjungimas	Techninio centro darbuotojas, atsakingas už oro kondicionavimo sistemos priežiūrą
			4.3.2. Kreipimasis į priežiūros tarnybą dėl pavojaus trukmės ir sutrikimo pašalinimo galimybių	Techninio centro darbuotojas, atsakingas už oro kondicionavimo sistemos priežiūrą
			4.3.3. Padarytos žalos likvidavimas (įrangos remontas, pakaitinės įrangos įsigijimas ar nuomas)	Atkūrimo grupė, techninio centro darbuotojas, atsakingas už oro kondicionavimo sistemos priežiūrą, išorinė priežiūros tarnyba
		4.4. Veiklos funkcijų atkūrimo vertinimas	4.4.1. Visiško funkcijų atkūrimo vertinimas, susijusių padalinių ir organizacijų informavimas	Valdymo grupė, Atkūrimo grupė
5.	Vandentiekio, nuotekų ir šildymo sistemų sutrikimai	5.1. Vandentiekio nuotekų ir / arba šildymo paslaugų teikėjų informavimas	5.1.1. Paslaugų teikėjų rekomendacijų gavimas	eLABa sisteminis administratorius, techninio centro darbuotojas, atsakingas už vandentiekio, nuotekų ir šildymo sistemų priežiūrą
		5.2. Sutrikimo šalinimo prognozės skelbimas	5.2.1. Darbuotojų informavimas, jei darbas esamose patalpose negali būti tęsiamas	Valdymo grupė, Atkūrimo grupė
			5.2.2. Paslaugų negaunančių padalinių ir organizacijų informavimas	Valdymo grupė, Atkūrimo grupė
			5.2.3. Darbo kitose patalpose ir nuotoliniu būdu organizavimas	Atkūrimo grupė

Eil. Nr.	Grėsmė	Pirminiai veiksmai	Pasekmių likvidavimo veiksmai	Atsakingi vykdytojai
		5.3. Sutrikimų pašalinimas	5.3.1. Padarytos žalos likvidavimas	Atkūrimo grupė, techninio centro darbuotojas, atsakingas už vandentiekio, nuotekų ir šildymo sistemų priežiūrą, išorinė priežiūros tarnyba
		5.4. Veiklos funkcijų atkūrimo vertinimas	5.4.1. Visiško funkcijų atkūrimo vertinimas, susijusių padalinių ir organizacijų informavimas	Valdymo grupė, Atkūrimo grupė
6.	Telekomunikacijų tinklų sutrikimas	6.1. Telekomunikacijų tinklų sutrikimo priežasčių nustatymas	6.1.1. Techninio centro vadovo ir susijusių tiekėjų informavimas	Atkūrimo grupės telekomunikacijų tinklų atsakingas specialistas, išorinė tarnyba
			6.1.2. Sprendimo dėl kitų tvarkytojų incidentų reagavimo grupių (CERT) informavimo priėmimas, informavimas	Valdymo grupė, Atkūrimo grupė
			6.1.3. Atsakingų kibernetinius incidentus valdančių ir tiriančių institucijų informavimas	Valdymo grupė, Atkūrimo grupė
			6.1.4. Paslaugų negaunančių padalinių ir organizacijų informavimas	Valdymo grupė, Atkūrimo grupė
		6.2. Telekomunikacijų tinklų sutrikimo šalinimas	6.2.1. Alternatyvių ryšių organizavimo poreikio ir galimybių vertinimas, pakaitinės įrangos nuoma ar įsigijimas	Atkūrimo grupės telekomunikacijų tinklų atsakingas specialistas, išorinė tarnyba
			6.2.2. Saugos incidento pasekmių likvidavimas	Atkūrimo grupės telekomunikacijų tinklų atsakingas specialistas, išorinė tarnyba

Eil. Nr.	Grėsmė	Pirminiai veiksmai	Pasekmių likvidavimo veiksmai	Atsakingi vykdytojai
		6.3. Veiklos funkcijų atkūrimo vertinimas	6.3.1. Visiško funkcijų atkūrimo vertinimas, susijusių padalinių ir organizacijų informavimas, incidento tyrimas	Valdymo grupė, Atkūrimo grupė
7.	Pagrindinių tarnybinių stočių sugadinimas ir (ar) praradimas	7.1. Pažeistų tarnybinių stočių nustatymas	7.1.1. Sistemų savininkų informavimas	Atkūrimo grupės vadovas, Atkūrimo grupė (specialistai)
			7.1.2. Atsakingų kibernetinius incidentus valdančių ir tiriančių institucijų informavimas	Valdymo grupė, Atkūrimo grupė
			7.1.3. Paslaugų negaunančių padalinių ir organizacijų informavimas	Valdymo grupė, Atkūrimo grupė
			7.1.4. Pažeistų stočių teikiamų paslaugų atkūrimas kitose patalpose	Atkūrimo grupės vadovas, Atkūrimo grupė (specialistai)
		7.2. Informacijos saugos priemonių plano sudarymas ir įgyvendinimas	7.2.1. Žalą likviduojančių darbuotojų instruktavimas	Atkūrimo grupės vadovas
			7.2.2. Minimalios apimties paslaugų atkūrimas	Atkūrimo grupės vadovas, Valdymo grupė, atsakingas administratorius
			7.2.3. Žalos įvertinimas, veiklos atkūrimo sąmatos sudarymas	Atkūrimo grupės vadovas, Valdymo grupė
			7.2.4. Žalos padarinių likvidavimas	Atkūrimo grupė, atsakingas sisteminis administratorius
		7.3. Veiklos funkcijų atkūrimo vertinimas	7.3.1. Visiško funkcijų atkūrimo vertinimas, susijusių padalinių ir organizacijų informavimas, incidento tyrimas	Valdymo grupė, Atkūrimo grupė

Eil. Nr.	Grėsmė	Pirminiai veiksmai	Pasekmių likvidavimo veiksmai	Atsakingi vykdytojai
8.	Pavojingas (įtartinas) radinys, teroristinė veikla	8.1.Teisėsaugos informavimas	8.1.1. Techninio centro apsaugos tarnybos informavimas	Radinį aptikęs darbuotojas, techninio centro darbuotojas, atsakingas už darbuotojų saugą ir sveikatą
			8.1.2. Poreikio evakuoti darbuotojus iš patalpų vertinimas	Techninio centro darbuotojas, atsakingas už darbuotojų saugą ir sveikatą
		8.2. Darbuotojų evakavimas	8.2.1. Darbuotojų informavimas apie evakuaciją	Techninio centro darbuotojas, atsakingas už darbuotojų saugą ir sveikatą
		8.3. Patalpų užrakinimas	8.3.1. Teisėsaugos nurodymų vykdymas	Techninio centro darbuotojas, atsakingas už darbuotojų saugą ir sveikatą
		8.4. Teisėsaugos nurodymų vykdymas	8.4.1. Darbuotojų informavimas apie nurodymų vykdymą	Atkūrimo grupės vadovas
		8.5. Veiksmai išlaisvinus užgrobtas patalpas	8.5.1. Padarytos žalos įvertinimas	Išorinė tarnyba, Atkūrimo grupė, Valdymo grupė
			8.5.2. Padarytos žalos likvidavimo priemonių plano sudarymas, paskelbimas, vykdymas	Atkūrimo grupė, Valdymo grupė
			8.5.3. Žalą likviduojančių darbuotojų instruktavimas	Atkūrimo grupės vadovas
		8.6. Veiklos funkcijų atkūrimo vertinimas	8.6.1. Visiško funkcijų atkūrimo vertinimas, susijusių padalinių ir organizacijų informavimas	Valdymo grupė, Atkūrimo grupė
9.	Nepasiekiami darbuotojai (dėl sveikatos sutrikimų, stichinių nelaimių ir nelaimingų atsitikimų)	9.1. Saugos incidento rizikos įvertinimas	9.1.1. Veiksmai pagal darbų saugos instrukcijas	Atkūrimo grupės vadovas, eLABa saugos įgaliotinis, techninio centro darbuotojas, atsakingas už darbuotojų saugą ir sveikatą

Eil. Nr.	Grėsmė	Pirminiai veiksmai	Pasekmių likvidavimo veiksmai	Atsakingi vykdytojai
		9.2. Pavaduojančių asmenų instruktavimas	9.2.1. Informacijos prieigos ribojimas, pakaitinio / pavaduojančio darbuotojo skyrimas.	eLABa naudotojų teisių administratorius, Atkūrimo grupė
			9.2.2. Trūkstamų darbuotojų paieška ir priėmimas į darbą	Nukentėjusio padalinio vadovas, Atkūrimo grupės vadovas
		9.3. Veiklos funkcijų atkūrimo vertinimas	9.3.1. Vertinama, ar visškai atkurtos funkcijos nukentėjusiame centre	Valdymo grupė, Atkūrimo grupė
10.	Institucijos duomenų vagystė	10.1. Pažeisto komponento izoliavimas	10.1.1. Incidentų reagavimo grupių (CERT) informavimas, pažeistų komponentų ir tinklo segmentų izoliavimas	Atkūrimo grupė, atsakingas už pažeistą segmentą administratorius
			10.1.2. Visuomenės ir duomenų subjektų, Valstybinės duomenų apsaugos inspekcijos ir Nacionalinio kibernetinio saugumo centro prie KAM informavimas	Atkūrimo grupės vadovas, eLABa saugos įgaliotinis
			10.1.3. Duomenų atstatymas, incidento tyrimas, kitų incidento pasekmių likvidavimas	Atkūrimo grupė
		10.2. Informacijos saugos priemonių plano sudarymas ir įgyvendinimas	10.2.1. Veiklos atkūrimo sąmatos sudarymas	Atkūrimo grupė, eLABa saugos įgaliotinis
		10.3. Veiklos funkcijų atkūrimo vertinimas	10.3.1. Vertinama, ar visiškai atkurtos funkcijos nukentėjusioje institucijoje	Valdymo grupė, Atkūrimo grupė

Lietuvos akademinės elektroninės
bibliotekos informacinės sistemos
veiklos tęstinumo valdymo plano
2 priedas

LIETUVOS AKADEMINĖS ELEKTRONINĖS BIBLIOTEKOS ELEKTRONINĖS INFORMACIJOS IR KIBERNETINIŲ SAUGOS INCIDENTŲ VALDYMO IR TYRIMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos akademinės elektroninės bibliotekos elektroninės informacijos ir kibernetinių saugos incidentų valdymo ir tyrimo tvarkos aprašas (toliau – Aprašas) reglamentuoja Lietuvos akademinės elektroninės bibliotekos informacinės sistemos (toliau – eLABa) naudotojų, valdytojo ir tvarkytojų darbuotojų veiksmus, įvykus elektroninės informacijos ir kibernetiniams saugos incidentams (toliau – saugos incidentai) ir jų sprendimo bei tyrimo tvarką.

II SKYRIUS
PRANEŠIMŲ APIE SAUGOS INCIDENTUS REGISTRAVIMAS IR NEATIDĖLIOTINI SAUGOS INCIDENTŲ PLĖTROS SUSTABDYMO VEIKSMAI

2. eLABa naudotojas apie saugos incidentus nedelsdamas praneša savo institucijos eLABa darbo vietų administratoriui.
3. eLABa darbo vietų administratorius praneša institucijos eLABa saugos įgaliotiniui.
4. Institucijos eLABa saugos įgaliotinis, vadovaudamasis Incidentų klasifikacija ir veiklos atkūrimo terminais (Plano 3 priedas), vertina saugos incidentą ir, pasitvirtinus įtarimui dėl saugos incidento, praneša eLABa pagrindiniam tvarkytojui IT pagalbos telefonu (8 5) 236 6200 darbo valandomis ir elektroniniu paštu pagalba@vu.lt ne darbo valandomis.
5. Gautas pranešimas apie saugos incidentą registruojamas adresu https://darbai.labt.lt/redmine skiltyje „eLABa incidentai“ ir priskiriamas eLABa pagrindiniam administratoriui ir eLABa sistemos administratoriui spręsti, informacinės sistemos priežiūrą vykdančio padalinio vadovui ir informacinės sistemos eLABa saugos įgaliotiniui stebėti.
6. Pagrindinis eLABa administratorius įvykus saugos incidentui:
6.1. atsižvelgdamas į veiklos tęstinumo detaliajame plane nustatytą poreikį informuoja kitus atsakingus asmenis;
6.2. kartu su eLABa administratoriais organizuoja saugos incidentų plėtros stabdymo veiksmus;
6.3. kartu su konsorciumo informacinių sistemų priežiūros darbo grupe (toliau – KISP grupė) sprendžia saugos incidentus;
6.4. jei kitaip nenuspręsta, organizuoja veiklos atstatymo po saugos incidentų veiklą;
6.5. kartu su KISP grupe renka medžiagą tirtiniems saugos incidentams;
6.6. informuoja atsakingus asmenis apie veiklos atstatymo eigą;
6.7. pagal poreikį eskaluoja saugos incidento kategoriją;
6.8. registruoja informaciją apie saugos incidento aplinkybes ir jo sprendimą IT pagalbos informacinėje sistemoje (prie pranešimo apie incidentą);
6.9. išsprendus saugos incidentą, pateikia išvadą tiesioginiam vadovui ir eLABa saugos įgaliotiniui žiniai;
6.10. priėmus sprendimą saugos incidentą uždaryti, informuoja pranešusį naudotoją;
6.11. išsprendus saugos incidentą, rengia rizikos mažinimo prevencinių priemonių planą;

6.12. vykdo įgaliotų asmenų nurodymus.

7. eLABa saugos įgaliotinis:

7.1. nustato pradinę saugos incidento kategoriją;

7.2. stebi saugos incidentų šalinimą;

7.3. organizuoja saugos incidentų tyrimą;

7.4. teikia nurodymus KISP grupė ir incidentų reagavimo grupėms (CERT) dėl tyrimui reikalingos medžiagos pateikimo;

7.5. renka tyrimui reikalingą medžiagą;

7.6. bendradarbiauja su incidentų reagavimo grupėmis (CERT) ir kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugos ir kibernetinius incidentus bei neteisėtas veiklas;

7.7. informuoja eLABa duomenų valdymo įgaliotinį apie saugos incidento tyrimo eigą;

7.8. teikia eLABa duomenų valdymo įgaliotiniui išvadą dėl prevencinių priemonių plano pakankamumo;

7.9. incidentų registracijos informacinėje sistemoje pateikia tyrimo metu nustatytą informaciją ir uždaro saugos incidentą, kai šis išsprendžiamas;

7.10. konsultuoja tiriant saugos incidentus kitus eLABa administratorius ir eLABa vidaus naudotojus.

8. Įtaręs neteisėtą veiklą, pažeidžiančią ar neišvengiamai pažeisiančią informacinės sistemos saugą, eLABa saugos įgaliotinis apie tai praneša eLABa duomenų valdymo įgaliotiniui ir kompetentingoms institucijoms, tiriančioms elektroninių ryšių tinklų, informacijos saugos ir kibernetinius incidentus, neteisėtas veiklas, susijusias su saugos incidentais.

III SKYRIUS
SAUGOS INCIDENTŲ TYRIMAS

9. Nereikšmingo poveikio saugos incidentų tyrimai neatliekami ir analizė Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos neteikiama. Tokiu atveju eLABa sistemos administratorius registruoja informaciją apie saugos incidento aplinkybes ir jo sprendimą adresu https://darbai.labt.lt/redmine skiltyje „eLABa incidentai“ ir pateikia su išvada pagrindiniam eLABa administratoriui bei eLABa saugos įgaliotiniui žiniai.

10. Nereikšmingo poveikio eLABa incidentų sprendimą sistemoje užbaigia tiesioginis padalinio, prižiūrinčio informacinę sistemą arba eLABa incidento paveiktą eLABa veikti būtiną infrastruktūrą, vadovas.

11. eLABa saugos įgaliotinis turi teisę priimti sprendimą tirti sprendžiamą arba papildomai tirti jau išspręstą nereikšmingo poveikio saugos incidentą.

12. eLABa saugos įgaliotinis, nustatęs aplinkybes, dėl kurių saugos incidentas gali turėti didesnių, nei manyta, padarinių, arba nustatęs, kad saugos incidento padariniai neatitinka numatytų kriterijų, turi teisę perkvalifikuoti saugos incidentą į kitą kategoriją.

13. Tiriant informacinės sistemos saugos incidentus, eLABa saugos įgaliotinis turi teisę gauti informaciją iš visų veiklos tęstinumo atstatyme dalyvavusių ir kitų galinčių turėti reikiamos informacijos darbuotojų bei tvarkytojų incidentų reagavimo grupių (CERT).

14. Vidutinio ir didesnio poveikio saugos incidentų tyrimas:

14.1. saugos incidentams tirti gali būti sudaromos specializuotos incidentų tyrimo grupės (toliau – Tyrimo grupė);

14.2. Tyrimo grupės narius eLABa saugos įgaliotinio siūlymu skiria techninių centrų ir, poreikiui esant, kitų tvarkytojų vadovai;

14.3. Tyrimo grupei vadovauja eLABa saugos įgaliotinis.

15. Siekdamas nustatyti saugos incidento aplinkybes, priežastis ir asmenis, dėl kurių galbūt neteisėtų veiksmų įvyko saugos incidentas, eLABa saugos įgaliotinis Tyrimo grupės nariams skiria saugos incidento tyrimo užduotis.

16. Tyrimo grupės nariai turi teisę:

16.1. apžiūrėti saugos incidento vietą;

16.2. apklausti su saugos incidentu galimai susijusius eLABa naudotojus;

16.3. susipažinti su saugos incidento tyrimui reikalingais dokumentais;

16.4. priimti sprendimą dėl saugos incidento kategorijos keitimo;

16.5. priima sprendimą dėl incidento rizikos mažinimo plano tinkamumo;

16.6. gauti kitą, su saugos incidentu susijusią informaciją.

17. Tyrimo grupė:

17.1. vadovaudamasi surinkta tyrimo medžiaga, surašo saugos incidento tyrimo išvadą, kurioje išdėsto saugos incidento aplinkybes, priežastis ir jas pagrindžiančius įrodymus, taip pat nurodo asmenis, dėl kurių neteisėtos veiklos įvyko saugos incidentas, ir šiuos duomenis teikia eLABa duomenų saugos įgaliotiniui;

17.2. vadovaudamasi Lietuvos akademinės elektroninės bibliotekos informacinės sistemos duomenų saugos nuostatais ir kitais saugos dokumentais pagal savo kompetenciją dalyvauja eLABa veiklos tęstinumo atkūrimo veiklose;

17.3. Valdymo grupės vadovo sprendimu bendradarbiauja su žalą likviduojančiomis specialiosiomis tarnybomis ir kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugos ir kibernetinius incidentus, neteisėtas veiklas, susijusias su saugos incidentais;

17.4. atsižvelgdama į saugos incidento padarinius, atlieka liekamosios rizikos vertinimą;

17.5. atsižvelgdama į saugos incidento priežastis ir jo padarinius, prireikus nedelsdama rengia Lietuvos akademinės elektroninės bibliotekos informacinės sistemos veiklos tęstinumo valdymo plano ar kitų eLABa saugos politiką įgyvendinančių dokumentų pakeitimo ar papildymo projektą.

18. Saugos incidentų registracijos žurnale nurodoma, kada saugos incidentas išspręstas ir kas padaryta atstatant veiklą.

19. Tyrimo ataskaitoje turi būti pateikta bent ši informacija: saugos incidento vieta, grėsmės kodas, saugos incidento aprašymas, pradžia (data ir laikas), pabaiga (data ir laikas), tyrimą vykdžiusių darbuotojų duomenys.

20. Surinkęs tyrimo medžiagą, eLABa saugos įgaliotinis pateikia apibendrinančią išvadą, priima sprendimą dėl saugos incidento tyrimo pabaigos ir informuoja eLABa duomenų valdymo įgaliotinį.

21. Saugos incidentų registracijos žurnalo išrašas, tyrimo medžiaga ir tyrimų ataskaitos pateikiami eLABa valdytojui arba pagrindiniam eLABa tvarkytojui pareikalavus, atitikties ir rizikos vertinimams vykdyti bei kitais LR įstatymų numatytais atvejais.

22. Saugos incidentų žurnalo ir tyrimų medžiaga saugoma ne trumpiau kaip 1 metus nereikšmingo bei vidutinio poveikio saugos incidentams ir 3 metus didelio poveikio bei pavojingiems saugos incidentams, po ko gali būti naikinama per 3 mėnesius pasibaigus kalendoriniams saugojimo termino metams.

IV SKYRIUS
BAIGIAMOSIOS NUOSTATOS

23. Ši tvarka skelbiama ta pačia tvarka kaip ir kiti informacinės sistemos dokumentai.

24. Asmenys, dėl kurių neteisėtų veiksmų ar neveikimo įvyko saugos incidentas, atsako teisės aktų nustatyta tvarka.

Lietuvos akademinės elektroninės
bibliotekos informacinės sistemos
veiklos tęstinumo valdymo plano
3 priedas

INCIDENTŲ KLASIFIKACIJA IR VEIKLOS ATKŪRIMO TERMINAI

I. KRITERIJAI, KURIAIS VADOVAUJANTIS SAUGOS INCIDENTAI PRISKIRIAMI KATEGORIJOMS

Nereikšmingas (N) (bent vienas iš kriterijų)				**Vidutinis (V)** (du ar daugiau kriterijų)					**Didelis (D)** (du ar daugiau kriterijų)				
Informacinė sistema netrikdoma, arba trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius mažiau nei 5 % visų registruotų sistemos naudotojų	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	Informacinė sistema trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar informacinės sistemos konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	Informacinė sistema trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 25 %	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar informacinės sistemos konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur

II. VEIKLOS ATKŪRIMO TERMINAI

Incidento kategorija	**Minimalaus funkcionalumo atkūrimo terminas**	**Visiško funkcionalumo atkūrimo terminas**
Pavojingas	5 d.	30 d.
Didelis	4 d.	15 d.
Vidutinis	3 d.	7 d.
Nereikšmingas	2 d.	5 d.

_____

Lietuvos akademinės elektroninės
bibliotekos informacinės sistemos
veiklos tęstinumo valdymo plano
4 priedas

VEIKLOS ATKŪRIMO PRIORITETAI

1. PIRMAS PRIORITETAS: INFRASTRUKTŪROS ATKŪRIMAS

Eil. Nr.	Sutrumpintas kodas	Infrastruktūros sistema
1.	I1	Fizinė sauga
2.	I2	Elektros maitinimas
3.	I3	Šaldymas
4.	I4	Kompiuterių tinklas ir susijusios paslaugos (virtualus privatus tinklas (VPN), telefonija)
5.	I5	Duomenų saugyklos
6.	I6	Serveriai
7.	I7	Duomenų kopijavimo ir atkūrimo sistema
8.	I8	Duomenų bazės
9.	I9	Sisteminio elektroninio pašto paslauga

2. ANTRAS PRIORITETAS: PRIORITETINIŲ PASLAUGŲ ATKŪRIMAS

Eil. Nr.	Sutrumpintas kodas	Paslauga	Priklauso nuo
1.	P1	eLABa aplikacijų, paieškos vartų programinė įranga*	I1−I9
2.	P2	eLABa apkrovos paskirstymo programinė įranga, eLABa svetainė*	I1−I8
3.	P3	eLABa administratorių darbo vietos	I1−I2, I4
4.	P4	eLABa Valdymo ir Atkūrimo grupių narių darbo vietos	I1−I2, I4

* Pastaba: paslaugos laikomos atkurtos minimalia konfigūracija, kai veikia sistemos eLABa naudotojų aplikacijos P1 (be ataskaitų) ir informacinės sistemos svetainė P2 (be ataskaitų).

_____

Lietuvos akademinės elektroninės
bibliotekos informacinės sistemos
veiklos tęstinumo valdymo plano
5 priedas

VEIKSMINGUMO IŠBANDYMO ATASKAITA

(data, dokumento numeris)

Plano išbandymo dalyviai:

Scenarijaus apibūdinimas:

Paslaugos ir sistemos, kuriuos paveikė scenarijus:

Išbandymo valdymo eiga:

Nustatyti trūkumai:

Pasiūlymai keisti arba papildyti Planą:

eLABa saugos įgaliotinis (vardas, pavardė)

(parašas)

Atkūrimo grupės vadovas (vardas, pavardė)

(parašas)

Valdymo grupės vadovas (vardas, pavardė)

(parašas)

_____

Pakeitimai:

1.
Lietuvos Respublikos švietimo, mokslo ir sporto ministerija, Įsakymas
Nr. V-1150, 2019-10-14, paskelbta TAR 2019-10-14, i. k. 2019-16303
Dėl Lietuvos Respublikos švietimo ir mokslo ministro 2015 m. liepos 2 d. įsakymo Nr. V-710 „Dėl Lietuvos akademinės elektroninės bibliotekos informacinės sistemos saugos politiką įgyvendinančių dokumentų patvirtinimo“ pakeitimo