LIETUVOS RESPUBLIKOS ŠVIETIMO, MOKSLO IR SPORTO MINISTRAS

ĮSAKYMAS
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

2019 m. spalio 14 d. Nr. V-1150
Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 43 straipsnio 2 dalimi, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 8 punktu,

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

1. pakeičiu nurodytuoju įsakymu patvirtintas Lietuvos akademinės elektroninės bibliotekos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisykles ir išdėstau jas nauja redakcija (pridedama);

2. pakeičiu nurodytuoju įsakymu patvirtintą Lietuvos akademinės elektroninės bibliotekos informacinės sistemos veiklos tęstinumo valdymo planą ir išdėstau jį nauja redakcija (pridedama);

3. pakeičiu nurodytuoju įsakymu patvirtintas Lietuvos akademinės elektroninės bibliotekos informacinės sistemos naudotojų administravimo taisykles ir išdėstau jas nauja redakcija (pridedama).

Švietimo, mokslo ir sporto ministras Algirdas Monkevičius

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

PATVIRTINTA
Lietuvos Respublikos švietimo ir mokslo ministro
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.

_____