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 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.

_____

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
			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	1.2.1. Darbuotojų, galinčių pavaduoti iš kito techninio centro arba dirbti nuotoliniu būdu iš kitų patalpų informavimas.	Valdymo grupė, Atkūrimo grupė

Eil. Nr.	Grėsmė	Pirminiai veiksmai	Pasekmių likvidavimo veiksmai	Atsakingi vykdytojai
		darbuotojų nuotolinėje vietoje instruktavimas	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
			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

Eil. Nr.	Grėsmė	Pirminiai veiksmai	Pasekmių likvidavimo veiksmai	Atsakingi vykdytojai
		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
			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

Eil. Nr.	Grėsmė	Pirminiai veiksmai	Pasekmių likvidavimo veiksmai	Atsakingi vykdytojai
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
		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

Eil. Nr.	Grėsmė	Pirminiai veiksmai	Pasekmių likvidavimo veiksmai	Atsakingi vykdytojai
		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
		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

Eil. Nr.	Grėsmė	Pirminiai veiksmai	Pasekmių likvidavimo veiksmai	Atsakingi vykdytojai
			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
		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

Eil. Nr.	Grėsmė	Pirminiai veiksmai	Pasekmių likvidavimo veiksmai	Atsakingi vykdytojai
			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
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,	9.1. Saugos incidento rizikos įvertinimas	9.1.1. Veiksmai pagal darbų saugos instrukcijas	Atkūrimo grupės vadovas, eLABa saugos įgaliotinis, techninio centro darbuotojas,

Eil. Nr.	Grėsmė	Pirminiai veiksmai	Pasekmių likvidavimo veiksmai	Atsakingi vykdytojai
	stichinių nelaimių ir nelaimingų atsitikimų)			atsakingas už darbuotojų saugą ir sveikatą
		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)

_____