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

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).

_____

_____