

**LIETUVOS NACIONALINĖS MARTYNO MAŽVYDO
BIBLIOTEKOS
MINIMALŪS KIBERNETINIO SAUGUMO REIKALAVIMAI**

**I SKYRIUS
BENDROSIO NUOSTATOS**

1. Šiuo dokumentu nustatomi minimalūs kibernetinio saugumo reikalavimai ir darbo principai (toliau – Reikalavimai), taikomi Lietuvos nacionalinei Martyno Mažvydo bibliotekai (toliau – LNB) paslaugas teikiantiems tiekėjams, taip pat jų pasitelktoms trečiosioms šalims, t. y. ūkio subjektams, kurių pajėgumais remiasi (toliau kartu – Tiekėjas, atskirai Tiekėjas ir Tiekėjo pasitelktos trečiosios šalys), veikiantiems LNB tinklų ir informacinėse sistemose (toliau – TIS). Reikalavimai taikomi neatsižvelgiant į paslaugų sutarties tipą ar jos vertę.

2. Neteisėto atskleidimo, korupcinio pobūdžio ir kitų neteisėtų veikų prevencijos, taip pat informacinių sistemų bei informacijos saugos ir Reikalavimų kontrolės bei paslaugų suteikimo kontrolės tikslu Tiekėjo veiksmai, atliekami jungiantis ir prisijungus prie LNB TIS, gali būti stebimi ir įrašomi.

3. Tiekėjas yra atsakingas už savo darbuotojų ir kitų Tiekėjo pasitelktų trečiųjų šalių darbuotojų, kurie turi prieigą prie LNB TIS ar gali būti susiję su prieigos prie LNB TIS suteikimu ar naudojimu, supažindinimą su Reikalavimais iki jiems suteikiant prieigą ir turi gebėti tai įrodyti.

4. Tiekėjas privalo užtikrinti ir kontroliuoti, kad jo darbuotojų ir kitų Tiekėjo pasitelktų trečiųjų šalių darbuotojų veiksmai, naudojama programinė ir aparatinė įranga nepažeis, neteisėtai nekeis ar kitaip nesutrikdys LNB TIS veiklos, nebus atskleista konfidenciali informacija, asmens duomenys ar padaryta žala LNB arba tretiesiems asmenims.

5. Tiekėjo darbuotojų ir kitų Tiekėjo pasitelktų trečiųjų šalių darbuotojų, kurie turi prieigą prie LNB TIS ar gali būti susiję su prieigos prie LNB TIS suteikimu ar naudojimu, informacinių technologijų ir informacijos saugos žinios turi būti pakankamos paslaugoms suteikti. Tiekėjas turi vertinti šių žinių lygį ir, jei reikia, organizuoti papildomus mokymus.

6. LNB pateikus oficialų prašymą ar įvykus reikšmingam incidentui, siekiant patvirtinti, jog Tiekėjas laikosi Reikalavimų, Tiekėjas suteikia LNB ar LNB pasirinktai trečiajai šaliai, veikiančiai LNB pavedimo pagrindu, leidimą atlikti visų Tiekėjo aplinkoje taikytų valdymo priemonių, susijusių su LNB duomenų tvarkymu ir (ar) paslaugų LNB teikimu, vertinimą, auditą, tikrinimą ar peržiūrą. Atliekant tokį vertinimą, Tiekėjas turi bendradarbiauti, t. y., suteikti galimybę susipažinti su kompetentingais darbuotojais, dokumentais, infrastruktūra ar bet kuria kita reikalinga informacija (duomenimis) bei programine įranga, kuri naudojama apdorojant, saugant ar perduodant LNB duomenis. LNB turi teisę atlikti neplaninį patikrinimą įvykus dideliame kibernetiniame incidentui. Reikiamą informaciją Tiekėjas pateikia ne vėliau kaip per 5 darbo dienas nuo LNB prašymo pateikimo dienos. Tuo atveju, jeigu patikrinimo metu nustatomi trūkumai, Tiekėjas privalo pašalinti rastus trūkumus per LNB nurodytą protingą terminą. Tiekėjas neturi teisės prieštarauti LNB nustatytam terminui.

7. LNB nepadengia jokių Tiekėjo išlaidų, kurias Tiekėjas patiria bendradarbiaudamas patikrinimo metu arba šalindamas nustatytus trūkumus.

8. Tiekėjas privalo nedelsiant, bet ne vėliau kaip per 4 valandas nuo momento, kai jam tapo žinoma, pranešti el. paštu infosauga@lnb.lt apie visus pastebėtus ar įtariamus kibernetinio saugumo incidentus ir įvykius bei Reikalavimų laikymosi pažeidimus (net jei jų faktas dar nėra patvirtintas), įskaitant, bet neapsiribojant, šiais įvykiais: nustatyta kenkėjiška programinė įranga, aptikta kibernetinė ataka ar įsilaužimas, pastebėtas pažeidžiamumas, prarasta įranga ar įrenginiai, kuriuose yra LNB informacija, neteisėtai atskleisti LNB duomenys, prarasti prisijungimo duomenys ir pan.

9. Tiekėjas ne vėliau kaip per 72 valandas nuo incidento nustatymo momento pateikia LNB kibernetinio incidento tyrimo ataskaitą. Jeigu incidentas įvyko Tiekėjo infrastruktūroje, jis privalo imtis visų reikiamų priemonių incidento suvaldymui ir galimų pasekmių sumažinimui.

II SKYRIUS

ĮRANGOS SAUGOS REIKALAVIMAI

10. Tiekėjas privalo užtikrinti, kad jo darbuotojai ir kitų Tiekėjo pasitelktų trečiųjų šalių darbuotojai prie LNB TIS jungtųsi iš įrenginių, kuriems būtų taikomos atitinkamos jų keliamai rizikai informacijos saugos priemonės, įskaitant, bet neapsiribojant, šias minimalias priemones:

10.1. turi būti naudojama gamintojų palaikoma aparatinė įranga, užtikrinant savalaikį naujausių aparatinės programinės įrangos saugos pataisų diegimą;

10.2. turi būti įdiegta antivirusinė programinė įranga, užtikrinant, kad antivirusinės programinės įrangos naujiniai būtų diegiami ne rečiau kaip kartą per parą;

10.3. turi būti nuolat diegiamos operacinės sistemos ir naudojamos programinės įrangos gamintojų išleistos kritinės ir svarbios saugos pataisos;

10.4. naudotojo ir administratorių paskyros turi būti atskirtos, t. y., administratorių paskyros naudojamos tik konfigūravimo ir kitiems administratoriaus teisių reikalaujantiems veiksmams atlikti;

10.5. naudojami slaptažodžiai turi atitikti Reikalavimų V skyriaus nuostatas;

10.6. turi būti aktyvuotas automatinis naudotojo paskyros užrakinimas, įsijungiantis ne vėliau kaip po 15 min. naudotojo neveiklumo;

10.7. turi būti įjungta ir naudojama kompiuterinės darbo vietos ugniasienė;

10.8. kompiuterinės darbo vietos vidinė atmintis turi būti užšifruota (pvz., naudojant „Bitlocker“ arba lygiavertę programinę įrangą);

10.9. naudojamos išorinės atminties laikmenos turi būti šifruojamos (pvz., naudojant „Bitlocker“ arba lygiavertę programinę įrangą).

11. Tiekėjas turi imtis deramų priemonių užtikrinant, kad LNB TIS aptarnavimui naudojama programinė įranga yra saugi ir tinkamai licencijuota. Draudžiama naudoti nelegalią, nelicencijuotą programinę įrangą.

12. LNB turi teisę, be išankstinio perspėjimo, blokuoti Tiekėjo turimą prieigą prie LNB TIS ar naudojamus įrenginius, jei nustatyta, kad Tiekėjo veiksmai ar naudojami įrenginiai kelia grėsmę LNB informacijai, LNB TIS veikimui, neatitinka Reikalavimų nuostatų arba Tiekėjo darbuotojų ar kitų Tiekėjo pasitelktų trečiųjų šalių darbuotojų elgesys LNB TIS infrastruktūroje kelia įtarimų arba gali sukelti grėsmes LNB informacijai arba TIS (pvz., DDoS atakos, šiukšlių pašto žinutės ir pan.).

13. Prieš suteikiant prieigą prie LNB TIS, LNB turi teisę patikrinti Tiekėjo darbo priemonių, su kuriomis ketinama jungtis prie LNB TIS, atitiktį Reikalavimų nuostatomis.

14. Tiekėjas privalo užtikrinti pažeidžiamumą, galinčių kelti riziką LNB TIS, valdymą, įskaitant savalaikį saugos pataisų diegimą, pažeidžiamumą stebėseną ir jų taisymą per LNB nurodytą protingą terminą. Tiekėjas neturi teisės prieštarauti LNB nustatytam terminui.

III SKYRIUS

IDENTIFIKAVIMO PRIEMONĖS IR RIBOJIMAI

15. Prisijungimo paskyros prie LNB TIS yra unikalios, jei tai neriboja techninės galimybės, ir suteikiamos asmeniškai tik Tiekėjo įgaliotiems asmenims.

16. Tiekėjas įsipareigoja užtikrinti, kad paskyrų naudotojai laikysis Reikalavimų, suteiktus prisijungimo duomenis naudos tik pagal tiesioginę paskirtį sutartoms paslaugoms atlikti, saugos paslapyje ir neatskleis tretiesiems asmenims. Tiekėjas privalo supažindinti paskyrų naudotojus su Reikalavimais.

17. Nustačius bet kokius sutarties, kuriai įgyvendinti buvo suteikta prieiga, ar Reikalavimų pažeidimus, suteikta prieiga gali būti nedelsiant panaikinama ir apie tokius veiksmus informuojamas Tiekėjas.

18. Tiekėjas privalo užtikrinti kelių veiksmų autentifikaciją (MFA) visose sistemose, kuriose tvarkomi LNB duomenys ar priemonės naudojamos prieigai prie LNB TIS, nepriklausomai nuo to, ar prieiga yra nuotolinė ar ne.

IV SKYRIUS

DARBO SU LNB TIS REIKALAVIMAI

19. Tiekėjas, teikdamas paslaugas, susijusias su LNB TIS, atsakingas už Reikalavimų laikymąsi, praktikų, užtikrinančių kibernetinį ir informacijos saugumą, taikymą. Jei Tiekėjas dėl informacijos stokos ar kitų priežasčių negali to užtikrinti, jis privalo nedelsdamas stabdyti teikiamas paslaugas ir nedelsdamas, bet ne vėliau kaip per 4 val. nuo fakto sužinojimo momento, apie tai pranešti LNB el. paštu infosauga@lnb.lt.

20. Paslaugas teikti leidžiama tik tokia apimtimi ir tik tokioje LNB TIS, kiek tai yra numatyta ar reikalauja sutartis, pateiktas užsakymas ar kita forma išreikštas LNB poreikis. Bet kokie kiti veiksmai turi būti suderinti su LNB darbuotojais, atsakingais už sutarties vykdymą, o jų nesuderintas atlikimas yra draudžiamas.

21. Dirbant su LNB TIS draudžiama:

21.1. savavališkai perduoti LNB TIS aparatinę įrangą naudoti tretiesiems asmenims;

21.2. savavališkai ardyti, remontuoti ar keisti LNB TIS aparatinės įrangos komplektaciją, jei tai nėra Paslaugų teikimo dalis ir tai nėra suderinta su LNB darbuotoju, atsakingu už TIS infrastruktūrą;

21.3. prie LNB TIS jungti nesankcionuotus duomenų perdavimo tinklo įrenginius (pvz., 3/4/5G ryšio modemus ir pan.), taip pat bet kokius kitus, tiesioginės paslaugų atlikimui neskirtus įrenginius;

21.4. LNB TIS diegti, saugoti ar joje paleisti nelicencijuotą, neautorizuotą programinę įrangą ar autorių teisėmis apsaugotus kūrinius ar juos naudoti pažeidžiant licencijavimo sąlygas ar autorių teises;

21.5. išnešti LNB TIS aparatinę įrangą, nesuderinus šių veiksmų su už atitinkamos sutarties vykdymą atsakingu LNB darbuotoju;

21.6. kopijuoti, saugoti, perduoti LNB informacinėse sistemose esančius duomenis ir informaciją į kitą, LNB nevaldoma infrastruktūrą, nesuderinus šių veiksmų su už atitinkamos sutarties vykdymą atsakingu LNB darbuotoju (pvz., draudžiama testavimo ar kitais tikslais perkelti duomenų bazes, sistemas ar kitus informacinius išteklius į paslaugos tiekėjo valdomą infrastruktūrą, kopijuoti LNB informaciją į failų mainų sistemas „WeTransfer“, „Google Drive“ ir pan.);

21.7. blokuoti, išjungti antivirusines programas, ugniasienę ir kitas LNB TIS naudojamas saugos priemones ar keisti jų nustatymus;

21.8. naudoti bet kokias priemones, įrangą ir paslaugas (pvz., tarpinius serverius (proxy), VPN, SSH tunelius, DNS tunelius ir pan.), siekiant apeiti LNB naudojamas saugos sistemas, pasiekti blokuojamus interneto išteklius ar paslaugas, atlikti kitus, su teikiamomis paslaugomis nesusijusius, veiksmus ar slėpti savo atliekamus veiksmus, išskyrus tuos atvejus, kai jų naudojimas yra reikalingas atlikti sutartyje numatytas funkcijas ir yra suderintas su LNB kibernetinio saugumo vadovu;

21.9. naudoti LNB TIS išteklius su teikiamomis paslaugomis nesusijusiais tikslais, komercinei veiklai, taip pat smurto, amoralaus elgesio skatinimui, įžeidžiančių pranešimų skleidimui ir pan. Tiekėjo ir Tiekėjo pasitelktų trečiųjų šalių darbuotojai privalo laikytis etikos normų ir atsako už informaciją, pateiktą naudojant LNB kompiuterinius tinklus;

- 21.10. užsiimti veikla, kuri pažeidžia Lietuvos Respublikos įstatymus;
- 21.11. nesankcionuotai naudotis svetimais ištekliais (pvz., dirbti kitam naudotojui suteiktais prisijungimo duomenimis, kopijuoti ir naudotis programomis ir duomenimis be išteklių savininko žinios ir sutikimo, jungtis prie kompiuterių be atitinkamo leidimo ir pan.);
- 21.12. savavališkai keisti LNB TIS parametrus, nesuderinus pokyčių su LNB darbuotoju, atsakingu už TIS infrastruktūrą (pvz., IP adresą, įrangos vardus ir pan.);
- 21.13. savo paslaugų teikimui skirtuose įrenginiuose naudoti programas, kurios apsunkina ar trikdo LNB TIS veikimą (pvz., tinklo ar sistemų skenavimo programos, tinklo ar sistemų blokavimo programos ir pan.);
- 21.14. vykdyti LNB TIS, taip pat kompiuterių tinklo, pažeidžiamumo skenavimą. Pažeidžiamumo skenavimo priemonių naudojimas galimas tik suderinus jų naudojimą su LNB kibernetinio saugumo vadovu.

V SKYRIUS

SLAPTAŽODŽIŲ SAUGOS REIKALAVIMAI

22. Reikalavimuose pateikti slaptažodžių saugos reikalavimai taikomi Tiekėjo ištekliams (įrenginiams ir sistemoms), kurie skirti aptarnauti LNB TIS ar jais yra tvarkoma LNB informacija.
23. Kiekvienam Tiekėjo ar Tiekėjo pasitelktos trečiosios šalies darbuotojui, jei neriboja techninės galimybės, suteikiamas unikalus, asmeninis prisijungimo prie LNB TIS vardas.
24. Tiekėjas privalo įpareigoti savo ir Tiekėjo pasitelktos trečiosios šalies darbuotojus saugoti jiems suteiktus prisijungimo duomenis, neperduoti jiems suteiktų prieigos teisių kitiems asmenims, įskaitant ir kitą Tiekėjo personalą. Tiekėjo ir kitų Tiekėjo pasitelktų trečiųjų šalių darbuotojai negali naudotis kitiems asmenims išduotais prisijungimo duomenimis.
25. Tiekėjas yra tiesiogiai atsakingas už visus Tiekėjo ir kitų Tiekėjo pasitelktų trečiųjų šalių darbuotojų prisijungimo vardu atliktus žalingus veiksmus ir LNB padarytus nuostolius.
26. Reikalavimai slaptažodžiams:
- 26.1. slaptažodžius draudžiama sudarinėti naudojant lengvai nuspėjamas sekas (pvz., qwerty, ABC123 ir pan.) ar naudoti asmeninio pobūdžio informaciją (pvz., gimimo data, šeimos narių vardai, įmonių pavadinimai ir pan.);
- 26.2. slaptažodžius turi sudaryti ne mažiau kaip 12 simbolių, kurių sudarymui turi būti panaudotos didžiosios ir mažosios raidės, skaičiai bei specialieji simboliai;
- 26.3. slaptažodžiai turi būti keičiami ne rečiau kaip kartą per tris mėnesius. Keičiant slaptažodį, turi būti užtikrinta, kad naujo slaptažodžio negalima nuspėti, žinant prieš tai buvusį slaptažodį.
27. Prisijungimo slaptažodžiai gali būti saugomi ar perduodami tik šifruotu pavidalu arba naudojant specialią slaptažodžių valdymui skirtą programinę įrangą (pvz., „KeePass“ arba lygiavertę). Draudžiama saugoti ar perduoti prisijungimo slaptažodžius nešifruotus, užrašytus atviru tekstu (pvz., popieriuje, failuose, programinėje įrangoje ir pan.).
28. Draudžiama prieigai prie LNB TIS naudojamus slaptažodžius naudoti kitur (pvz., internetinėse sistemose, asmeninio naudojimo sistemose arba įrenginiuose, kitų kliento įrenginiuose ir pan.).
29. Kai dėl techninių ar organizacinių ribojimų būtina taikyti slaptažodžių sudėtingumo išimtis, turi būti gautas LNB kibernetinio saugumo vadovo, patvirtinimas ir įgyvendintos papildomos priemonės, skirtos sumažinti informacijos saugos rizikas, kylančias dėl taikomos išimties.

VI SKYRIUS

TEISIŲ SUTEIKIMO REIKALAVIMAI

30. Tiekėjas turi nedelsdamas, bet ne vėliau nei per 24 valandas informuoti apie savo ir kitų Tiekėjo pasitelktų trečiųjų šalių darbuotojų darbo ir kitų sutarčių nutraukimą ir kitus

pakeitimus, siekiant užtikrinti, kad prieiga prie LNB TIS būtų panaikinta ir (ar) išduota įranga būtų grąžinta ne vėliau kaip paskutinę sutarties su tais asmenimis galiojimo dieną.

31. Iki paslaugų teikimo pradžios Tiekėjas turi būti įdiegęs formalią procedūrą prieigos teisių suteikimui ir panaikinimui ir ją taikyti prieigos prie LNB TIS valdymui ir, LNB pareikalavus, ją pateikti.

32. Tiekėjo prieigos valdymo formali procedūra turi apimti ir užtikrinti šių reikalavimų laikymąsi:

32.1. pasirašytos sutarties, kurios įgyvendinimas reikalauja prieigos suteikimo, pagrindu, ne ilgesniam, negu reikia, sutartinių įsipareigojimų įvykdymo terminui ir mažiausia konkrečioms veiksmams atlikti reikalinga apimtimi;

32.2. pasirašius konfidencialumo įsipareigojimą;

32.3. Tiekėjas užtikrina, kad asmenų, kuriems Tiekėjas suteikė prieigą prie savo informacinių išteklių, naudojamų LNB paslaugoms teikti prieigos teisės būtų panaikinamos ne vėliau kaip paskutinę sutarties ar paslaugų, kurioms suteikti buvo reikalinga prieiga, teikimo dieną;

32.4. įpareigojimai trečiąją šalį laikytis reikalavimų, atitinkančių šiuos Reikalavimus.

VII SKYRIUS

NUOTOLINĖS PRIEIGOS REIKALAVIMAI

33. Nuotolinei prieigai prie LNB TIS galima naudoti tik LNB suteiktus prisijungimo metodus ir priemones. Savavališka nuotolinė prieiga prie LNB TIS griežtai draudžiama. Nuotolinė prieiga suteikiama tik tais atvejais, kai tai yra būtina sutartyje numatytoms paslaugoms suteikti.

34. Nuotolinis prisijungimas prie LNB TIS per viešuosius tinklus (internetą), realizuojamas tik naudojant LNB VPN.

35. Nesankcionuotas LNB VPN naudojimas sutartyje nenumatytais tikslais griežtai draudžiamas.

36. VPN naudotojai atsako už tai, kad negaliojantieji (neautorizuoti) asmenys VPN prisijungimo sesijos metu neprieitų prie LNB TIS (pvz., paliekant savo darbo vietą, privaloma atsijungti nuo LNB VPN, aktyvuoti kompiuterio ekrano užrakimo funkcija ir pan.).

37. Nuotolinė prieiga suteikiama Tiekėjui arba ir kitoms Tiekėjo pasitelktoms trečiosioms šalims tik:

37.1. pateikus nuotolinės prieigos gavėjo pasirašytą konfidencialumo pasižadėjimą;

37.2. pateikus Tiekėjo įgalioto asmens nuotolinės prieigos prie LNB išteklių prašymą;

37.3. atsakingas už sutarties vykdymą LNB darbuotojas nuotolinės prieigos užsakymą pateikia LNB savitarnoje (<https://pagalba.lnb.lt>) kartu su prieigos gavėjo konfidencialumo pasižadėjimu;

37.4. prieiga suteikiama paslaugų teikimo sutarties galiojimo laikotarpiui.

38. Tiekėjas, prisijungęs prie LNB TIS, privalo laikytis šių Reikalavimų nuostatų.

VIII SKYRIUS

PASLAUGŲ TEIKIMO LYGMENYS IR TIEKĖJŲ SAUGOS

VALDYMAS

39. Tiekėjas privalo užtikrinti ir dokumentuoti paslaugų teikimo lygmenis (SLA), susijusius su kibernetiniu saugumu.

40. Tiekėjas turi turėti kibernetinių incidentų valdymo planą, kuris turi būti pateikiamas LNB, esant poreikiui.

41. Tiekėjas, naudodamas Tiekėjo pasitelktas trečiąsias šalis paslaugoms, susijusioms su LNB TIS, teikti, privalo:

41.1. užtikrinti, kad Tiekėjo pasitelktoms trečiosioms šalims būtų taikomi ne mažesni kibernetinio saugumo reikalavimai nei nustatyti šiuo dokumente;

41.2. pranešti LNB apie subtiekėjų pakeitimus iš anksto, bet ne vėliau kaip per 30 kalendorinių dienų;

41.3. užtikrinti LNB teisę patvirtinti arba atmesti esminius subtiekėjų pakeitimus.

IX SKYRIUS

ŠALIŲ TEISĖS IR ATSAKOMYBĖ

42. LNB turi teisę bet kuriame sutarties vykdymo etape tikrinti, kaip Tiekėjas laikosi Reikalavimų nuostatų, įskaitant, bet neapsiribojant, Tiekėjo prisijungimui prie LNB TIS naudojamų darbo priemonių atitiktis Reikalavimams tikrinimą be išankstinio įspėjimo.

43. Tiekėjas atsako už žalą, kilusią dėl Reikalavimų nesilaikymo, įskaitant trečiųjų šalių patirtus nuostolius. LNB turi teisę reikalauti žalos atlyginimo Lietuvos Respublikos teisės aktų nustatyta tvarka.

44. Kibernetinio saugumo reikalavimų pažeidimai laikomi esminiu sutarties pažeidimu, suteikiančiu LNB teisę vienašališkai nutraukti sutartį su Tiekėju, įspėjus ne mažiau kaip prieš 10 darbo dienų, išskyrus atvejus, kai pažeidimas kelia tiesioginę grėsmę LNB TIS.

45. Tiekėjas įsipareigoja Reikalavimų pažeidimų atveju bendradarbiauti su LNB ir kompetentingomis institucijomis (Nacionaliniu kibernetinio saugumo centru prie Krašto apsaugos ministerijos ir kt.), pateikdamas visą reikiamą informaciją ir sudarydamas sąlygas tinkamam incidento tyrimo atlikimui.
