**LIETUVOS NACIONALINĖS MARTYNO MAŽVYDO BIBLIOTEKOS KIBERNETINIO SAUGUMO REIKALAVIMAI TAIKOMI PROGRAMINĖS ĮRANGOS KAIP PASLAUGOS PIRKIMAMS**

## I SKYRIUS
## BENDROSIOS NUOSTATOS

1. Lietuvos nacionalinės Martyno Mažvydo bibliotekos (toliau – LNB) kibernetinio saugumo reikalavimai taikomi programinės įrangos kaip paslaugos pirkimams (toliau – Reikalavimai) nustato privalomus kibernetinio saugumo reikalavimus, taikomus programinės įrangos kaip paslaugos teikėjams, teikiantiems šias paslaugas LNB.

2. LNB yra priskirtas prie esminių kibernetinio saugumo subjektų pagal Lietuvos Respublikos kibernetinio saugumo įstatymą (toliau – KSĮ).

3. Reikalavimai parengti vadovaujantis Lietuvos Respublikos Kibernetinio saugumo įstatymo (toliau – KSĮ), Lietuvos Respublikos Vyriausybės nutarimo Nr. 818 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo patvirtinimo“ (toliau – Aprašas), LNB vidinių teisės aktų, reglamentuojančių kibernetinį saugumą, nuostatomis ir gerąja kibernetinio saugumo užtikrinimo praktika.

4. Reikalavimai yra neatskiriama kiekvieno pirkimo techninės specifikacijos, pagal kurią teikėjas teikia programinę įrangą kaip paslaugą LNB, dalis.

5. Reikalavimuose vartojamos sąvokos:

5.1. **programinė įranga kaip paslauga** (angl. Software as a Service, SaaS) (toliau – SaaS paslaugos) – debesų kompiuterijos paslaugų teikimo modelis, kuriame paslaugų teikėjas teikia programinę įrangą kaip paslaugą, valdydamas jos infrastruktūrą ir vykdydamas jos priežiūrą, o LNB darbuotojai ja naudojasi interneto naršyklės pagalba ar naudodami programinę sąsają (angl. API);

5.2. **Teikėjas** – ūkio subjektas, teikiantis SaaS paslaugas LNB pagal sutartį;

5.3. **SLA** – paslaugų teikimo lygio susitarimas (angl. Service Level Agreement).

6. Kitos Reikalavimuose vartojamos sąvokos atitinka KSĮ, Aprašo bei LNB vidinių teisės aktų, reglamentuojančių kibernetinį saugumą, sąvokas.

## II SKYRIUS
## BENDRI SAUGUMO REIKALAVIMAI

7. LNB valdomi duomenys turi būti tvarkomi ir saugomi Europos Sąjungos ir (arba) Europos ekonominės erdvės teritorijoje esančiuose duomenų centruose. Asmens duomenų perdavimas į Jungtines Amerikos Valstijas (JAV) leidžiamas tik tuo atveju, jei asmens duomenis JAV gaunantis duomenų valdytojas ar duomenų tvarkytojas yra galiojančiai sertifikuotas pagal EU–US Data Privacy Framework (DPF), laikosi DPF principų ir taiko visas pagal Bendrąjį duomenų apsaugos reglamentą numatytas tinkamas apsaugos priemones. LNB pareikalavus Teikėjas privalo pateikti galiojančio sertifikavimo įrodymus.

8. Duomenų centrų, kuriuose laikomi LNB duomenys, fizinė apsauga turi atitikti tarptautiniu mastu pripažintus standartus. LNB pareikalavus Teikėjas privalo pateikti duomenų centro fizinės ir aplinkos apsaugos atitikties įrodymą – duomenų centro operatoriaus sertifikatą (ISO/IEC 27001, SOC 2 Type II, Tier III ar lygiavertį) arba lygiavertę auditoriaus ataskaitą.

9. SaaS paslaugos turi būti dubliuojamos mažiausiai dviejuose geografiškai nutolusiuose duomenų centruose, siekiant užtikrinti SaaS paslaugos prieinamumą.

10. Teikėjas privalo užtikrinti SaaS paslaugos prieinamumą ne mažiau kaip 99 procentų laiko per sutarties galiojimo laikotarpį. Planinis SaaS paslaugos stabdymas derinamas su LNB atsakingu už sutarties vykdymą darbuotoju ne vėliau kaip prieš 3 darbo dienas.

11. Teikėjas privalo pateikti išsamų sąrašą visų subteikėjų ir trečiųjų šalių, dalyvaujančių teikiant SaaS paslaugą, nurodant jų atliekamas funkcijas ir prieigos prie LNB duomenų lygį;

12. Teikėjas privalo nedelsiant informuoti LNB apie bet kokius subteikėjų pokyčius, galinčius turėti įtakos teikiamos SaaS paslaugos saugumui.

13. LNB arba jos įgaliotas paslaugų teikėjas turi teisę atlikti Teikėjo atitikties šiems Reikalavimams auditą, įskaitant neplaninį, sutarties vykdymo laikotarpiu arba įvykus dideliam kibernetiniam incidentui. Teikėjas privalo sudaryti sąlygas tokiam auditui atlikti, tai yra užtikrinti kompetentingų darbuotojų dalyvavimą, suteikti prieigą prie dokumentų, infrastruktūros ir kitos audito atlikimui reikalingos informacijos bei programinės įrangos. Teikėjas reikiamą informaciją pateikia ne vėliau kaip per 5 darbo dienas nuo LNB rašytinio prašymo pateikimo dienos. Tuo atveju, jeigu patikrinimo metu nustatomi trūkumai, Teikėjas privalo juos pašalinti per LNB nurodytą protingą terminą.

14. LNB nepadengia jokių Teikėjo išlaidų, kurias Teikėjas patiria bendradarbiaudamas patikrinimo metu arba šalindamas nustatytus trūkumus.

15. Teikėjas privalo užtikrinti, kad SaaS paslaugos teikimui paskirti darbuotojai turėtų pakankamą kibernetinio saugumo srities kvalifikaciją. LNB pareikalavus, Teikėjas privalo pateikti informaciją apie SaaS paslaugos teikimui paskirtų darbuotojų turimus profesinius sertifikatus, baigtas mokymo programas ar kitą kvalifikaciją patvirtinančius dokumentus.

16. Teikėjas ir jo darbuotojai, taip pat Teikėjo pasitelktos trečiosios šalys ir jų darbuotojai, turintys prieigą prie LNB duomenų ar SaaS paslaugos administravimo aplinkos, privalo laikytis konfidencialumo reikalavimų.

## III SKYRIUS
## ATSARGINĖS KOPIJOS IR DUOMENŲ SAUGUMAS

17. Teikėjas privalo turėti dokumentuotą ir reguliariai testuojamą veiklos tęstinumo ir atkūrimo po incidentų planą, kuris turi būti pateiktas susipažinimui pagal atskirą LNB pareikalavimą.

18. Teikėjas privalo užtikrinti LNB valdomų duomenų atskyrimą, logiškai izoliuotą duomenų saugojimo aplinką, garantuojant, kad vieno kliento duomenys nebūtų prieinami ar nepaveiktų kito kliento duomenų.

19. Teikėjas privalo užtikrinti reguliarų LNB duomenų atsarginių kopijų darymą pagal šiuos minimalius reikalavimus:

19.1. atsarginės kopijos daromos ne rečiau kaip kartą per parą;

19.2. atsarginės kopijos saugomos geografiškai nutolusioje vietoje, atskirai nuo pagrindinės sistemos;

19.3. atsarginių kopijų duomenys šifruojami, o šifravimo raktai saugomi atskirai nuo kopijų;

19.4. atsarginės kopijos turi būti apsaugotos nuo keitimų (angl. immutable) užtikrinant, kad atsarginės kopijos negali būti modifikuotos, perrašytos ar ištrintos tiek vidinių procesų, tiek išorinių grėsmių (pvz., išpirkos reikalaujančių programų) atveju;

19.5. atsarginių kopijų atkūrimas testuojamas ne rečiau kaip kartą per pusę metų;

19.6. paslaugos atkūrimo laikotarpio tikslas (angl. Recovery Time Objective, RTO) – ne ilgiau kaip 8 valandos;

19.7. duomenų praradimo laikotarpio tikslas (angl. Recovery Point Objective, RPO) – ne daugiau kaip 24 valandos.

20. Pasibaigus sutarčiai arba ją nutraukus Teikėjas privalo suteikti LNB galimybę eksportuoti visus LNB duomenis elektronine forma, kurios formatai suderinami su LNB darbuotoju atsakingu už sutarties vykdymą.

21. Visi LNB duomenys, esantys Teikėjo infrastruktūroje, turi būti saugiai sunaikinti ne vėliau kaip per 30 kalendorinių dienų nuo sutarties pabaigos, sunaikinimo faktą fiksuojant rašytiniu patvirtinimu.

## IV SKYRIUS
## ŠIFRAVIMAS IR RYŠIO SAUGA

22. Visi duomenų perdavimo tinklu perduodami duomenys turi būti apsaugoti naudojant TLS protokolą, ne žemesnės kaip 1.3 versijos. Duomenų perdavimas nenaudojant šifravimo (HTTP, FTP ir pan.) yra draudžiamas. Teikėjas privalo realizuoti TLS 1.3 protokolo versiją ne vėliau kaip per 6 mėnesius nuo sutarties pasirašymo dienos.

23. LNB duomenys ramybės būsenoje (angl. data at rest) turi būti šifruojami naudojant visuotinai pripažintus saugius algoritmus (pvz., AES-256 ar lygiavertis).

24. Skaitmeniniai TLS sertifikatai turi būti išduoti patikimų sertifikavimo tarnybų.

## V SKYRIUS
## NAUDOTOJŲ TAPATYBĖS VALDYMAS IR AUTENTIFIKAVIMAS

25. Siekiant užtikrinti tinkamą LNB naudotojų valdymą, Teikėjui rekomenduojama taikyti integraciją su LNB valdoma tapatybės atpažinties sistemą (angl. Identity Provider) (toliau – IdP) Microsoft Entra ID, naudojant SAML 2.0 ar OpenID Connect protokolus, o nesant tokios galimybės realizuoti kelių faktorių autentifikavimo (angl. Multi-Factor Authentication) (toliau – MFA) sprendimą, kurio reikalavimai nurodyti šio skyriaus 23-24 punktuose.

26. Realizuota IdP integracija turi užtikrinti:

26.1. naudotojų prisijungimą per LNB valdomą Microsoft Entra ID paskyrą naudojant vienkartinį prisijungimą (angl. Single Sign-On, SSO);

26.2. automatinį naudotojų teisių suteikimą ir panaikinimą pagal LNB Microsoft Entra ID grupes, naudojant SCIM protokolą ar lygiavertį automatizuotą sprendimą;

26.3. draudimą naudotojams jungtis prie SaaS paslaugos naudojant lokalias paslaugos paskyras, kai įgalinta Microsoft Entra ID integracija. Išimtys gali būti taikomos tik techninėms (sisteminėms) paskyroms ar nesant galimybės taikyti IdP integracijos.

27. Tais atvejais, kai netaikoma ar nepalaikoma IdP integracija, Teikėjas privalo užtikrinti kelių faktorių autentifikavimą (MFA) kaip privalomą autentifikavimo priemonę.

28. Teikėjo realizuotas MFA turi palaikyti bent vieną iš šių metodų:

28.1. autentifikavimo programėlės generuojami vienkartiniai kodai (pvz., Microsoft Authenticator ar lygiaverčiai);

28.2. vienkartinių prisijungimo kodų siuntimas el. paštu ar mobiliojo ryšio trumpąja žinute (SMS);

28.3. naudojant Lietuvos Respublikos Elektroninių valdžios vartų portalą, palaikantį naudotojų autentifikavimą naudojant Smart-ID, mobilųjį parašą ar kitas portale realizuotas elektroninės atpažinties priemones.

29. Po ne daugiau kaip 5 iš eilės nesėkmingų bandymų autentifikuoti naudotoją, jo paskyra turi būti automatiškai blokuojami arba inicijuojamas papildomas patikrinimas.

30. Teikėjas privalo užtikrinti, kad Teikėjo darbuotojai, turintys administracinę prieigą prie LNB duomenų ar SaaS paslaugos valdymo aplinkos, naudotų unikalias, asmenines paskyras. Naudotojams suteiktos prieigos teisės turi atitikti mažiausios privilegijos principą ir apimti tik konkrečioms funkcijoms atlikti reikalingą prieigą.

31. Teikėjas privalo užtikrinti savalaikį Teikėjo darbuotojų, turinčių administracinę prieigą prie LNB duomenų ar SaaS paslaugos valdymo aplinkos, panaikinimą.

## VI SKYRIUS
## ŽURNALINIAI ĮRAŠAI

32. Teikėjas privalo užtikrinti, kad paslaugoje būtų fiksuojami ir saugomi bent šie žurnaliniai įrašai, susiję su LNB naudotojų veiksmais ir SaaS paslaugos administravimu:

32.1. naudotojų ir administratorių autentifikavimo įvykiai (sėkmingi ir nesėkmingi);

32.2. naudotojų paskyrų sukūrimas, pakeitimai ir panaikinimas;

32.3. administratorių atliekami veiksmai;

32.4. prieigos teisių suteikimas ir panaikinimas;

32.5. sistemos konfigūracijos pakeitimai;

32.6. saugumo pranešimai ir įspėjimai;

32.7. duomenų eksporto ir masinio atsisiuntimo operacijos.

33. Žurnaliniai įrašai saugomi ne trumpiau kaip 12 mėnesių. Jų vientisumas turi būti apsaugotas – įrašai negali būti keičiami ar trinami.

34. LNB pareikalavus, Teikėjas suteikia prieigą prie žurnalinių įrašų, susijusių su LNB duomenimis, per ne ilgesnį kaip 5 darbo dienų terminą.

## VII SKYRIUS
## PROGRAMINĖS ĮRANGOS SAUGA IR ATNAUJINIMAI

35. SaaS paslauga turi būti projektuojama pagal „saugumo užtikrinimo projektavimo metu“ (angl. Security by Design) principus, užtikrinant, kad saugumo sprendimai būtų integruoti į SaaS paslaugą jos kūrimo ir viso gyvavimo ciklo metu.

36. Teikėjas privalo užtikrinti, kad sutarties galiojimo laikotarpiu naudojama programinė įranga, platformos komponentai ir jų priklausomybės būtų palaikomos gamintojų. Pasenusios, gamintojų nebepalaikomos programinės įrangos naudojimas yra draudžiamas.

37. Teikėjas privalo užtikrinti SaaS paslaugos saugumo spragų stebėseną ir savalaikį jų šalinimą, vadovaujantis tarptautiniu mastu pripažintomis kibernetinio saugumo praktikomis.

38. Teikėjas privalo užtikrinti, kad SaaS paslaugos atnaujinimai būtų valdomi taip, kad nekeltų papildomų saugumo rizikų.

39. Teikėjas privalo turėti formalizuotą SaaS paslaugos pažeidžiamumų stebėsenos ir atskleidimo tvarką.

## VIII SKYRIUS
## KIBERNETINIŲ INCIDENTŲ VALDYMO REIKALAVIMAI

40. Teikėjas privalo turėti ir vykdyti reagavimo į kibernetinius incidentus procedūrą, nustatančią aiškią incidentų identifikavimo, klasifikavimo, šalinimo ir komunikavimo tvarką.

41. Teikėjas turi užtikrinti, kad LNB būtų informuojamas apie bet kokį saugumo incidentą, paveikusį ar galintį paveikti LNB duomenis ar SaaS paslaugos prieinamumą, laikantis šių terminų:

41.1. nedelsiant, bet ne vėliau kaip per 8 valandas nuo momento, kai Teikėjui tapo žinoma apie incidentą – pirminis perspėjimas, kuriame nurodomas incidento pobūdis, apimtis ir galimas poveikis LNB duomenims;

41.2. ne vėliau kaip per 24 valandas nuo momento, kai Teikėjui tapo žinoma apie incidentą – išsamesnis pranešimas, kuriame nurodoma:

41.2.1. incidento pobūdis ir mastas;

41.2.2. potencialus poveikis LNB duomenims;

41.2.3. taikomos korekcinės priemonės;

41.2.4. numatomas atkūrimo laikas.

42. Teikėjas privalo pateikti išsamią dokumentaciją po kiekvieno saugumo incidento, apimančią incidento analizę, priežastis ir priemones, kurių imtasi, siekiant išvengti panašių incidentų ateityje.

43. Teikėjas įsipareigoja 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.

## IX SKYRIUS
## PASLAUGŲ TEIKIMO KRITERIJAI

44. SaaS paslaugai taikomi paslaugų teikimo lygmenų (SLA) reikalavimai:

44.1. paslaugos prieinamumas – ne mažiau kaip 99 proc. laiko;

44.2. paslaugos sutrikimų registravimas 24 valandas per parą, 7 dienas per savaitę;

44.3. reagavimą į kibernetinius incidentus įprastomis ir nedarbo valandomis (esminio subjekto reikalavimas pagal Aprašo 36.1–36.2 punktus);

44.4. apsaugos nuo paslaugos trikdymo atakų (angl. Denial of Service, DoS) taikymą.

## X SKYRIUS
## ŠALIŲ ATSAKOMYBĖS

45. Teikėjo ir LNB atsakomybės kibernetinio saugumo srityje paskirstomos taip:

45.1. Teikėjas yra atsakingas už SaaS paslaugos kibernetinę saugą, duomenų apsaugą Teikėjo infrastruktūroje ir šiuose Reikalavimuose nustatytų prievolių vykdymą;

45.2. LNB yra atsakinga už savo naudotojų prieigos valdymą, tinkamą SaaS paslaugos naudojimą ir LNB pusėje taikomų saugumo priemonių įgyvendinimą;

45.3. Teikėjas neatsako už saugumo incidentus, kilusius dėl LNB naudotojų neteisėtų ar neapdairių veiksmų, jeigu Teikėjas įrodys, kad jo infrastruktūroje taikytos visos šiuose Reikalavimuose nustatytos apsaugos priemonės.

46. LNB turi teisę bet kuriame sutarties vykdymo etape tikrinti, kaip Teikėjas laikosi Reikalavimų nuostatų.

_____