ANTIVIRUSINĖS PROGRAMINĖS ĮRANGOS LICENCIJŲ TIEKIMO SUTARTIS Nr. _____

2023 m. spalio 20 d.
Vilnius

Lietuvos nacionalinė Martyno Mažvydo biblioteka, juridinio asmens kodas 290757560, adresas Gedimino pr. 51, 01109 Vilnius, atstovaujama [redacted] veikiančio pagal generalinio direktoriaus 2023-01-05 įsakymu Nr. B-5 patvirtintas Lietuvos nacionalinės Martyno Mažvydo bibliotekos finansų kontrolės taisykles (toliau – **Pirkėjas**), ir **UAB „NBCS“**, juridinio asmens kodas 301817848, adresas Šeškinės Sodų g. 12-54, LT-08343 Vilnius, atstovaujama [redacted], veikiančio pagal bendrovės įstatus (toliau – **Tiekėjas**), (toliau Sutartyje kartu vadinama Šalimis, kiekviena atskirai Šalimi), sudarė šią Sutartį.

1. SUTARTIES OBJEKTAS

1.1. Tiekėjas įsipareigoja Sutartyje numatytomis sąlygomis perduoti **Antivirusinės programinės įrangos licencijos** (toliau – Prekės) Pirkėjui nuosavybės teise, o Pirkėjas įsipareigoja priimti Prekes ir sumokėti už jas Tiekėjui Sutartyje nurodytomis sąlygomis ir terminais.
1.2. BVPŽ kodas 48761000-0.
1.3. Prekių kiekiai nurodyti Sutarties Priede Nr. 1 (Techninėje specifikacijoje).
1.4. Reikalavimai Prekėms ir jų įvykdymo sąlygos pateiktos Techninėje specifikacijoje (Sutarties 1 priedas).
1.1. Prekės atitinka Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo, patvirtinto Lietuvos Respublikos aplinkos apsaugos ministro 2011 m. birželio 28 d. įsakymu Nr. D1-508 (2022 m. gruodžio 13 d. įsakymo Nr. D1-401 redakcija), 4.4.3. punktą: perkama tik nematerialaus pobūdžio (intelektinė) ar kitokia paslauga, nesusijusi su materialaus objekto sukūrimu, kurios teikimo metu nėra numatomas reikšmingas neigiamas poveikis aplinkai, nesukuriamas taršos šaltinis ir negeneruojamos atliekos.

2. PREKIŲ KAINA IR ATSISKAITYMO TVARKA

2.1. Pradinės sutarties vertė sudaro **11.858,00 Eur (vienuolika tūkstančių aštuoni šimtai penkiasdešimt aštuoni eurai, 00 ct)**, įskaitant PVM. Pradinę Sutarties vertę sudaro:
2.1.1. Prekių vertė – 9.800,00 (devyni tūkstančiai aštuoni šimtai eurų, 00 ct), neįskaitant PVM;
2.1.2. Pridėtinės vertės mokestis (PVM) – 21 % (dvidešimt vienas procentas) 2.058,00 Eur (du tūkstančiai penkiasdešimt aštuoni eurai, 00 ct).
2.2. Į šią sumą įskaičiuoti visi mokesčiai ir visos Tiekėjo išlaidos, susijusios su šios Sutarties vykdymu, taip pat ir PVM bei PVM sąskaitos faktūros teikimo mokestis per „E. sąskaita“ sistemą.
2.3. Pradinė sutarties vertė (įkainiai) dėl pasikeitusio kainų lygio, mokesčių yra neperskaičiuojami.
2.4. Vadovaujantis Viešųjų pirkimų tarnybos direktoriaus patvirtinta kainodaros taisyklių nustatymo metodika, taikomas kainos apskaičiavimo būdas – fiksuota kaina.
2.5. Už Prekes, kurias Tiekėjas suteikia be Pirkėjo rašytinio sutikimo, Pirkėjas Tiekėjui neapmoka.
2.6. Visi mokėjimai ir atsiskaitymai pagal Sutartį vykdomi Lietuvos Respublikos nacionaline valiuta – eurais.
2.7. Tiekėjas PVM sąskaitas faktūras privalo pateikti LR VPĮ 22 straipsnio 3 dalyje nustatyta tvarka[1].
2.8. Pirkėjas sumoka Tiekėjui už faktiškai ir kokybiškai patiektas Prekes per 30 (trisdešimt) kalendorinių dienų nuo PVM sąskaitos faktūros[2] gavimo dienos. Jei Pirkėjas atsisako apmokėti pateiktą sąskaitą, jis pateikia motyvuotą raštišką atsisakymą tai atlikti.
2.9. PVM sąskaitoje faktūroje ar kito tipo priklausančiame išrašyti dokumente turi būti nurodytos atskirai patiektų Prekių ir su jomis susijusių paslaugų ir (ar) darbų kainos / įkainiai. Pateikus PVM sąskaitą faktūrą ar kito tipo priklausantį išrašyti dokumentą be atskirai patiektų Prekių ir su jomis susijusių paslaugų ir (ar) darbų kainų / įkainių, Pirkėjas turi teisę nepriimti tokios sąskaitos ir jos neapmokėti.
2.10. Pirkėjas turi ne vėliau kaip per 5 (penkias) darbo dienas nuo Tiekėjo raštiško kreipimosi pasirašyti Prekių perdavimo–priėmimo aktą, jei Prekių kokybė atitinka Sutartyje nustatytus reikalavimus. Jeigu Prekių perdavimo – priėmimo metu nustatoma, kad Prekės neatitinka Sutartyje nustatytų reikalavimų, Pirkėjas turi teisę atsisakyti pasirašyti Prekių perdavimo–priėmimo aktą, raštu nurodydamas priimto sprendimo motyvus.
2.11. Pirkėjas, nesumokėjęs Tiekėjui už Prekes per Sutartyje nurodytą terminą, Tiekėjui pareikalavus, moka Tiekėjui 0,05 procento nuo laiku nesumokėtos sumos dydžio delspinigius už kiekvieną uždelstą dieną.
2.12. Jei Tiekėjui pagal šią Sutartį yra priskaičiuotos netesybos ar taikoma kitokio pobūdžio civilinė

[1] Dėl elektroninių sąskaitų faktūrų. – Viešųjų pirkimų tarnyba (vpt.lt)
[2] Ar kito tipo priklausančio išrašyti Pirkėjui pateikti dokumento, atitinkančio PVM sąskaitos faktūros turinį ir tikslą.

atsakomybė, kurios taikymą numato Sutartis, Pirkėjo už Prekes mokėtina suma mažinama priskaičiuotų netesybų ir (arba) kitokios pritaikytos civilinės atsakomybės formos suma. Jeigu Pardavėjui už Prekes buvo sumokėta iš anksto, netesybos ar kitokio pobūdžio civilinė atsakomybė turi būti sumokėtos per 10 (dešimt) kalendorinių dienų nuo joms apmokėti išrašyto dokumento, kuriame pateikiamas reikalavimas sumokėti netesybas, gavimo dienos.

3. TIEKĖJO TEISĖ PASITELKTI TREČIUOSIUS ASMENIS (SUBTEIKIMAS)

3.1. Tiekėjas Sutarčiai vykdyti turi pasitelkti tik tuos subtiekėjus, kurie numatyti Tiekėjo pasiūlyme. Jeigu subtiekėjai nėra žinomi, nenurodyti Tiekėjo pasiūlyme, tokie subtiekėjai gali būti pasitelkiami Sutarties vykdymo metu, jei atitinka Pirkimo dokumentuose nustatytus reikalavimus (jei subtiekėjams buvo taikomi kvalifikaciniai reikalavimai ar tikrinamas pašalinimo pagrindų nebuvimas) ir tik gavus Pirkėjo pritarimą raštu.
3.2. Subtiekėjų pasitelkimas nekeičia Tiekėjo atsakomybės dėl Sutarties įvykdymo. Tiekėjas prisiima atsakomybę už subtiekėjų veiklą vykdant Sutartį ir atsako už sutartinių prievolių neįvykdymą ar netinkamą įvykdymą.
3.3. Jei Tiekėjas pakeičia esamą arba pasitelkia (pasamdo, įdarbina, leidžia tiekti Prekes pagal Sutartį ar kita) naują subtiekėją, negavęs Pirkėjo raštiško sutikimo, Tiekėjas, Pirkėjui pareikalavus, privalo sumokėti 5 (penkių) procentų nuo pradinės Sutarties vertės dydžio baudą ir šie subtiekėjai toliau negali tiekti Prekių.

4. PREKIŲ KOKYBĖ

4.1. Prekės ir Prekių kokybė turi atitikti Sutartyje ir Techninėje specifikacijoje (jei yra) bei teisės aktuose tokios Prekėms nustatytus reikalavimus.
4.2. Tiekėjo parduodamos Prekės privalo būti gamintojo pakuotėje[3], naujos, nenaudotos, tinkamos naudoti pagal jų tikslinę paskirtį, be paslėptų Prekių trūkumų, dėl kurių Prekių nebūtų galima naudoti pagal jų tikslinę paskirtį arba dėl kurių sumažėtų Prekių naudingumas.
4.3. Prekėms suteikiamas 12 mėnesių garantijos terminas, skaičiuojamas nuo Prekių perdavimo–priėmimo akto pasirašymo dienos.
4.4. Prekių perdavimo–priėmimo ar garantinio laikotarpio metu pastebėtiems trūkumams šalinti nustatomas 7 (septynių) kalendorinių dienų terminas. Prekių trūkumais laikomi nustatyti neatitikimai Techninėje specifikacijoje (jei yra), Sutartyje nustatytiems reikalavimams ar neatitikimai teisės aktų nuostatoms arba jeigu Prekių (ar jos vnt.) negalima naudoti pagal tikslinę paskirtį.
4.5. Tiekėjas per Sutarties 4.4 punkte nustatytą terminą nuo Pirkėjo pranešimo apie trūkumų nustatymą išsiuntimo dienos privalo savo jėgomis ir lėšomis pašalinti trūkumus. Už nustatytų Prekių trūkumų nepašalinimą per Sutarties 4.4 punkte nustatytą terminą, Tiekėjas, Pirkėjui pareikalavus, moka 0,05 procento nuo nepatiektų Prekių ir (ar) neįvykdytų kitų Tiekėjo įsipareigojimų vertės dydžio delspinigius už kiekvieną uždelstą dieną.
4.6. Jeigu tiekiant Prekes buvo teikiamos ir paslaugos ir (ar) atliekami darbai, kurių metu buvo naudojamos Tiekėjo perkamos medžiagos, už tokių medžiagų kokybę Tiekėjas atsako kaip pardavėjas pagal tiekimo sutartį.
4.7. Tiekėjas, tiekdamas Prekes, užtikrina saugos darbe, priešgaisrinės saugos, aplinkos apsaugos bei kitų teisės aktų nustatytų reikalavimų, taikomų tiekiant Prekes, laikymąsi (jei taikoma).

5. PREKIŲ PRISTATYMO TERMINAI IR PERDAVIMO – PRIĖMIMO TVARKA

5.1. Tiekėjas įsipareigoja Prekes pristatyti per 5 (penkias) darbo dienas nuo užsakymo pateikimo dienos.
5.2. Prekių pristatymo vieta – Gedimino pr. 51, Vilnius.
5.3. Rašytiniu Šalių sutarimu Prekių pristatymo ir (ar) Prekių trūkumų šalinimo terminai gali būti pratęsti arba sustabdyti, jeigu Tiekėjas, nesibaigus Sutartyje nustatytam Prekių pristatymo ir (ar) trūkumų šalinimo terminui, pateikia Pirkėjui argumentuotą prašymą ir šį prašymą pagrindžiančius dokumentus pratęsti Prekių tiekimo ir (ar) trūkumų šalinimo terminą, ir (ar) sustabdyti Sutarties vykdymą ir jame nurodytos aplinkybės yra susijusios bent su viena iš šių aplinkybių:
5.3.1. Pirkėjas nevykdo ar netinkamai vykdo savo įsipareigojimus pagal šią Sutartį ir todėl Tiekėjas negali tiekti Prekių laiku ir pateikiami šias aplinkybes patvirtinantys dokumentai;
5.3.2. Pirkėjo Tiekėjui pateikiami papildomi nurodymai ir (arba) informacija turi įtakos Tiekėjo Prekių tiekimo terminams ir pateikiami šias aplinkybes patvirtinantys dokumentai;
5.3.3. ypač nepalankios meteorologinės sąlygos turi įtakos Tiekėjo Prekių tiekimo terminams;

[3] Netaikoma, jei Prekės pagal savo pobūdį nėra įpakuojamos, ir (ar) jei perkama ne visa pakuotė.

5.3.4. valstybės ar savivaldos institucijų veiksmai arba bet kokios kitos kliūtys, priskirtinos Pirkėjui ir (arba) Pirkėjo samdomiems tretiesiems asmenims, trukdo Tiekėjui laiku patiekti Prekes ir pateikiami šias aplinkybes patvirtinantys dokumentai.
5.4. Sutarties 5.3 punkte numatytais atvejais Prekių pristatymo ir (ar) Prekių trūkumų šalinimo terminai gali būti pratęsiami ne ilgiau nei tęsiasi Sutarties 5.3 punkte nurodytos aplinkybės. Bet koks Sutarties keitimas dėl aukščiau nurodytų priežasčių yra pasirašomas raštu.
5.5. Jei Tiekėjas dėl savo kaltės nepristato Prekių (ar jų dalies) Sutarties 5.15.1 punkte nustatytais terminais, Tiekėjas moka 0,05 procento nuo nepristatytų / vėluojamų pristatyti Prekių ir (ar) neįvykdytų kitų Tiekėjo įsipareigojimų vertės dydžio delspinigius už kiekvieną uždelstą dieną ir atlygina Pirkėjo dėl to patirtus tiesioginius nuostolius tiek, kiek jų nepadengia netesybos (delspinigiai ir (ar) baudos).

6. ŠALIŲ TEISĖS IR PAREIGOS

6.1. **Tiekėjas įsipareigoja:**
6.1.1. patiekti Prekes pagal Sutartyje ir Techninėje specifikacijoje (jei ji yra) nustatytus reikalavimus, taip pat atitinkančias Lietuvos Respublikos įstatymų bei kitų norminių teisės aktų tokioms Prekėms keliamus reikalavimus, Prekių techninius aprašymus, tinkamas naudoti pagal Prekių įsigijimo paskirtį;
6.1.2. prisiimti Prekių atsitiktinio žuvimo ar sugedimo riziką iki Prekių pristatymo vietos, taip pat Prekių sugadinimo riziką iškrovimo metu iš Tiekėjo transporto (jei Prekes pristato ir iškrauna Tiekėjas ar jo pasitelkti Subtiekėjai) Pirkėjo nurodytoje Prekių pristatymo vietoje;
6.1.3. konsultuoti Pirkėją kitais, su Tiekėjo sutartiniais įsipareigojimais susijusiais, klausimais;
6.1.4. užtikrinti, kad Sutartį vykdys tik teisę verstis atitinkama veikla turintys asmenys, neatsižvelgiant į tai, ar Tiekėjo kvalifikacija dėl teisės verstis atitinkama veikla buvo tikrinama arba tikrinama ne visa apimtimi.
6.2. **Tiekėjas turi teisę:**
6.2.1. prašyti, kad Pirkėjas pateiktų su tinkamu Sutarties vykdymu susijusią informaciją ar dokumentus, kurių pateikimo būtinybė atsirado Sutarties vykdymo metu;
6.2.2. reikalauti, kad Pirkėjas tinkamai ir laiku vykdytų kitus sutartinius įsipareigojimus.
6.3. **Pirkėjas įsipareigoja:**
6.3.1. Tiekėjui tinkamai įvykdžius sutartinius įsipareigojimus, priimti patiektas Prekes;
6.3.2. Sutarties vykdymo metu bendradarbiauti su Tiekėju, teikiant Sutarties vykdymui pagrįstai reikalingą Pirkėjo turimą informaciją, kurios pateikimo būtinybė iškilo Sutarties vykdymo metu.
6.4. Kiti Pirkėjo ir Tiekėjo įsipareigojimai, teisės ir pareigos, apibrėžiami galiojančiuose Lietuvos Respublikos teisės aktuose, Sutartyje ir (ar) jos prieduose (jei apibrėžiami).

7. INTELEKTINĖS NUOSAVYBĖS TEISĖS

7.1. Visi rezultatai ir su jais susijusios teisės, įgytos vykdant Sutartį, įskaitant intelektinės nuosavybės teises, išskyrus asmenines neturtines teises į intelektinės veiklos rezultatus, yra Pirkėjo nuosavybė, pereinanti Pirkėjui nuo Prekių perdavimo – priėmimo momento be jokių apribojimų, kurią Pirkėjas gali naudoti, publikuoti, perleisti ar perduoti be atskiro Tiekėjo sutikimo tretiesiems asmenims.
7.2. Sutarties įgyvendinimo metu intelektinės nuosavybės teisių įgyvendinimas ir užtikrinimas vykdomas pagal Lietuvos Respublikos teisę.

8. SUTARTIES PAŽEIDIMAS IR JO PASEKMĖS, SUTARTIES NUTRAUKIMAS

8.1. Jei Šalis nevykdo arba netinkamai vykdo savo įsipareigojimus pagal Sutartį, ji pažeidžia Sutartį.
8.2. Sutartyje nustatytų netesybų dydis yra laikomas minimalia neginčijama nukentėjusiosios Šalies patirtų nuostolių suma, kurią kita Šalis turi kompensuoti nukentėjusiajai Šaliai dėl Sutarties pažeidimo (nesilaikymo), nereikalaujant nuostolių dydį patvirtinančių įrodymų.
8.3. Pirkėjas turi teisę vienašališkai, nesikreipdamas į teismą, prieš 5 (penkias) kalendorines dienas raštu apie tai įspėjęs Tiekėją, nutraukti Sutartį, jeigu Tiekėjas iš esmės pažeidė Sutartį. Tiekėjo padarytas Sutarties pažeidimas laikomas esminiu, jeigu Prekės neatitinka Sutartyje ir (ar) Techninėje specifikacijoje numatytų reikalavimų ir (ar) Tiekėjas neištaiso Prekių trūkumų per Sutartyje nustatytą terminą; Tiekėjo kvalifikacija tapo nebeatitinkančia šios Sutarties reikalavimų; Tiekėjui yra iškeliama bankroto ar restruktūrizavimo byla, arba bankroto procesas vykdomas ne teismo tvarka, inicijuotos priverstinio likvidavimo ar susitarimo su kreditoriais procedūros arba jam vykdomos analogiškos procedūros pagal šalies, kurioje jis registruotas, įstatymus; jei Tiekėjas dėl savo kaltės negali ir (arba) atsisako vykdyti Sutartyje numatytus įsipareigojimus ar bet kokią jų dalį, nepriklausomai nuo tokios dalies vertės; yra kitos aplinkybės, numatytos Lietuvos Respublikos civilinio kodekso 6.217 straipsnyje ar LR VPĮ 90 straipsnyje.

8.4. Pirkėjas bet kuriame Sutarties vykdymo etape turi teisę vienašališkai be iš ankstinio Tiekėjo įspėjimo nutraukti Sutartį, jeigu paaiškėja, kad tolesnis Sutarties vykdymas gali kelti grėsmę nacionaliniam saugumui arba paaiškėja, kad Tiekėjas, subtiekėjas, ūkio subjektas, kurio pajėgumais remiasi, gamintojas ar juos kontroliuojantys asmenys Lietuvos Respublikos Vyriausybės nutarimu pripažinti nepatikimais.
8.5. Sutartis gali būti nutraukiama raštišku abiejų Šalių sutarimu. Toks Šalių susitarimas turi būti įformintas papildomu susitarimu.
8.6. Sutarties pasibaigimas ar nutraukimas neturi įtakos ginčų nagrinėjimo tvarką nustatančių ir kitų Sutarties sąlygų galiojimui, jeigu šios sąlygos pagal savo esmę išlieka galioti ir po Sutarties pasibaigimo, t. y. kokybės garantijos, atsakomybės ir pan. Taip pat išlieka galioti visi atsiradę ir tinkamai neįvykdyti Salių tarpusavio įsipareigojimai, įskaitant, tačiau ne tik finansiniai įsipareigojimai.

9. ŠALIŲ ATSAKOMYBĖ

9.1. Nė viena iš Šalių neatsako už visišką ar dalinį įsipareigojimų nevykdymą, jeigu ji įrodo, kad įsipareigojimų neįvykdė dėl nenugalimos jėgos (*force majeure*) aplinkybių. Nenugalimos jėgos (*force majeure*) aplinkybės suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos civilinio kodekso 6.212 straipsnyje. Dėl atleidimo nuo atsakomybės esant nenugalimos jėgos aplinkybėms, Šalys vadovaujasi Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 (Žin., 1996, Nr. 68-1652). Nenugalima jėga (*force majeure*) nelaikoma tai, kad rinkoje nėra reikalingų prievolei vykdyti prekių, Sutarties Šalis neturi reikiamų finansinių išteklių arba Šalies kontrahentai pažeidžia savo prievoles.
9.2. Nenugalimos jėgos (*force majeure*) aplinkybės pratęsia Sutarties įsipareigojimų vykdymo terminus, tačiau, jei šios aplinkybės tęsiasi ilgiau nei 3 (tris) mėnesius nuo jų atsiradimo momento arba jeigu apie jas nėra laiku pranešta, ir Šalys nesutaria, kaip toliau bus vykdomi Sutarties nevykdžiusios Šalies įsipareigojimai, tuomet kita Šalis, raštu pranešusi ne mažiau kaip prieš 15 (penkiolika) kalendorinių dienų, turi teisę nutraukti šią Sutartį.

10. SUTARTIES ĮSIGALIOJIMAS, GALIOJIMAS IR KEITIMAS

10.1. Ši Sutartis įsigalioja jos pasirašymo dieną ir galioja 12 mėnesių.
10.2. Paskutinis Sutarties galiojimo mėnuo yra skirtas ne Prekių tiekimui, o apmokėjimui už patiektas Prekes.
10.3. Sutartis gali baigti galioti anksčiau, jei Sutarties įgyvendinimo metu bus pasiekta pradinė Sutarties vertė arba patiektos Sutartyje numatytos Prekės.
10.4. Sutarties sąlygos jos galiojimo laikotarpiu gali būti keičiamos neatliekant naujos pirkimo procedūros vadovaujantis šios Sutarties nuostatomis ir (ar) LR VPĮ 89 straipsnio nuostatomis ir užtikrinant, kad nebūtų pažeisti šio įstatymo 17 straipsnyje nustatyti principai ir tikslai. Sutarties sąlygų pakeitimai įforminami Šalių rašytiniais susitarimais, kurie yra neatsiejama Sutarties dalis.

11. KITOS SĄLYGOS

11.1. Šalys negali perduoti savo teisių ir pareigų dėl visos ar dalies šios Sutarties trečiosioms šalims be raštiško kitos Šalies sutikimo.
11.2. Tiekėjas, pasirašydamas šią Sutartį įsipareigoja vadovautis, 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Reglamentas), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu ir Valstybinės duomenų apsaugos inspekcijos rekomendacijomis.
11.3. Ši Sutartis, jos priedai ir atlikti Sutarčių pakeitimai, išskyrus informaciją, kuri pagal teisės aktus yra laikoma konfidencialia, nėra laikomi konfidencialiais ir bus viešinami Centrinėje viešųjų pirkimų informacinėje sistemoje.
11.4. Šalys susitaria laikyti informaciją, kuri pagal teisės aktus yra laikoma konfidencialia, paslaptyje neterminuotai, neatsižvelgiant į tai, ar ta informacija pateikiama žodžiu ar raštu. Šalys susitaria neatskleisti konfidencialios informacijos, kuri pagal teisės aktus yra laikoma konfidencialia, jokiai trečiai šaliai be išankstinio raštiško ją pateikusios Šalies sutikimo, taip pat nenaudoti tokio pobūdžio konfidencialios informacijos asmeniniams ar trečiųjų asmenų poreikiams, išskyrus atvejus, kai tokia informacija turi būti atskleista pagal teisės aktų reikalavimus.
11.5. Kiekviena Šalis privalo per 5 (penkias) darbo dienas pranešti kitai Šaliai apie Sutartyje nurodytų adreso, rekvizitų, kontaktinių asmenų, banko sąskaitos pasikeitimą. Iki informavimo apie adreso pasikeitimą, visi šioje Sutartyje nurodytu adresu išsiųsti pranešimai ir kita korespondencija laikomi įteiktais tinkamai.
11.6. Visus Šalių tarpusavio santykius, atsirandančius iš šios Sutarties ir neaptartus jos sąlygose, reglamentuoja Lietuvos Respublikos įstatymai ir kiti teisės aktai.

11.7. Visus ginčus dėl šios Sutarties vykdymo Šalys įsipareigoja spręsti derybomis. Jeigu Šalys šių ginčų negali išspręsti derybomis, jie sprendžiami Lietuvos Respublikos teismuose teisės aktų nustatyta tvarka.
11.8. Ši Sutartis sudaryta dviem vienodą teisinę galią turinčiais egzemplioriais, po vieną kiekvienai Šaliai.
11.9. Šalys susitaria, jog ši Sutartis gali būti sudaroma nuotoliniu būdu Šalims tarpusavyje apsikeičiant pasirašytomis ir (PDF ir kitame formate) skenuotomis elektroninėmis Sutarčių (teksto) versijomis. Šalies parašas skenuotoje elektroninėje Sutarties versijoje patvirtina, jog Šalis tinkamai išreiškė valią sudaryti Sutartį joje nurodytomis sąlygomis. Šalys susitaria, jog šiame punkte numatyta tvarka ir forma sudaryta Sutartis yra laikoma galiojančia ir teisiškai įpareigoja abi Šalis.
11.10. Pirkėjo paskirtas asmuo, atsakingas už Sutarties ir pakeitimų paskelbimą pagal LR VPĮ 86 straipsnio 9 dalies nuostatas yra Teisės ir žmogiškųjų išteklių skyriaus darbuotojas.
11.11. Už Sutarties tinkamą vykdymą atsakingi:

[redacted]

12. PRIEDAI

12.1. Kiekvienas šios Sutarties priedas yra neatskiriama jos dalis. Kiekviena Šalis gauna po vieną kiekvieno Sutarties priedo egzempliorių.
12.2. Prie Sutarties pridedami šie priedai:
12.2.1. Priedas Nr. 1 – Techninė specifikacija.
12.2.2. Priedas Nr. 2 – Pasiūlymas.

13.ŠALIŲ REKVIZITAI

Tiekėjas: **UAB „NBCS“** Įmonės kodas: 301817848 Adresas: Šeškinės Sodų g. 12-54, LT-08343 Vilnius Tel. 8 606 23260 El. p. info@nbcs.lt Ats. sąsk. Nr. LT332140030003850923 Bankas: Luminor Bank AS Lietuvos skyrius Banko kodas: 40100 PVM mokėtojo kodas: LT100006470618	**Pirkėjas:** **Lietuvos nacionalinė Martyno Mažvydo biblioteka** Įstaigos kodas: 290757560 Adresas: Gedimino pr. 51, 01109 Vilnius Tel. (8 5) 249 7023 El. p. biblio@lnb.lt Ats. sąsk. Nr. LT78 7044 0600 0128 4138 Bankas: AB SEB bankas Banko kodas: 70440 PVM mokėtojo kodas: LT100000031710
[redacted] _____ A.V.	[redacted] A.V.

TECHNINĖ SPECIFIKACIJA ANTIVIRUSINEI PROGRAMINEI ĮRANGAI

1. SPECIFIKACIJA TIPINIŲ DARBO VIETŲ IR TARNYBINIŲ STOČIŲ APSAUGAI

Eil. Nr.	Parametras	Minimali reikšmė
1.	Licencijų skaičius	300 vnt.
2.	Programinės įrangos tipas	Kompiuterinių darbo vietų, serverių, mobiliųjų ir planšetinių įrenginių, apsauga nuo virusų ir šnipinėjimo programų, su ugniasiene, bei apsauga nuo elektroninių šiukšlių. Visi programinės įrangos sprendimai privalo būti valdomi iš vienos administravimo konsolės debesijoje. Turi būti galimybė administravimo konsolę diegti organizacijos viduje.
3.	Programinės įrangos gamintojas	Turi būti nurodytas. Visi pateikti apsaugos nuo virusų bei el. šiukšlių produktai turi būti pagaminti to paties gamintojo.
4.	Programinės įrangos paketo pavadinimas	Turi būti nurodytas.
5.	Palaikomos operacinės sistemos	Kompiuterinės darbo vietos: *Microsoft Windows 11 32-bitų ir 64-bitų.* *Microsoft Windows 10 32-bitų ir 64-bitų.* *macOS 10.12 ir naujesnės.* *Ubuntu Desktop 20.04 LTS.* *Ubuntu Desktop 22.04 LTS.* *Red Hat Enterprise Linux 7, 8 su įdiegta palaikoma darbalaukio aplinka.* *SUSE Linux Enterprise Desktop 15.* *Linux Mint 20.* Mobilieji įrenginiai: *Android 6 ir naujesnės.* *iOS 9 ir naujesnės.* *iPadOS 13 ir naujesnės.* Windows serveriai: *Microsoft Windows Server 2022 (Server Core ir Desktop Experience).*

		Microsoft Windows Server 2019 (įskaitant Server Core, Desktop Experience ir Essentials). *Microsoft Windows Server 2016 (įskaitant Server Core, Desktop Experience, Storage Server ir Essentials).* *Microsoft Windows Server 2012 R2 (įskaitant Storage Server ir Essentials).* *Server Core (Microsoft Windows Server 2012 R2).* Linux serveriai: *RedHat Enterprise Linux (RHEL) 7, 8 ir 9 versijos.* *CentOS 7 versijos.* *Ubuntu Server 20.04 LTS ir 22.04 LTS versijos.* *Debian 10 ir 11 versijos.* *SUSE Linux Enterprise Server (SLES) 12 ir 15 versijos.* *Oracle Linux 8 versijos.* *Amazon Linux 2 versijos.* Turi būti palaikomos virtualios aplinkos: *Microsoft Hyper-V Server 2012 ir naujesnė.* *VMware vSphere/ESXi 6.5 ir naujesnė.* *VMware Workstation 9 ir naujesnė.* *VMware Player 7 ir naujesnė.* *Oracle VirtualBox 6.0 ir naujesnė.* *Citrix 7.0 ir naujesnė.* Sprendimas su VMware ESXi turi palaikyti *VMware* Horizon 7.x ir 8.0 versijas. Nuotolinio administravimo konsolė turi palaikyti (diegiant organizacijos viduje): *Microsoft Windows Server 2012 R2 64-bitų.* *Microsoft Windows Server 2012 R2 Core 64-bitų.* *Microsoft Windows Storage Server 2012 R2 64-bitų.* *Microsoft Windows Server 2016 64-bitų.* *Microsoft Windows Storage Server 2016 64-bitų.* *Microsoft Windows Server 2019 64-bitų.*

		Microsoft Windows Server 2022 64-bitų. *Linux: RHEL, Debian, Ubuntu, SLED, SLES, OpenSUSE, Fedora ir CentOS bei dauguma kitų RPM ir DEB paketų valdymu pagrįstų platinamų programų.* Nuotolinė administravimo konsolė turi būti suderinama su naršyklėmis: • *Mozilla Firefox.* • *Microsoft Edge.* • *Google Chrome.* • *Opera.* • *Safari.*
6.	Veikimo kokybės reikalavimai	Programinės įrangos gamintojas turi turėti ISO 9001:2015 ir ISO 27001:2013 arba lygiaverčius standartus atitinkančias sertifikacijas. Siūlomo produkto gamintojas turi būti *Leaders* arba *Challengers* kategorijose 2022 metų "Gartner Magic Quadrant for Endpoint Protection Platforms". Gamintojas turi būti įvertintas „TOP Player" įvertinimu 2023 metų "Radicati Endpoint Security Market Quadrant" rinkos tyrime. „AV-TEST" verslo produktų apžvalgos ir sertifikavimo ataskaitoje gamintojo saugumo sprendimai, skirti „Windows", turi būti įvertinti „TOP Product" įvertinimu, remiantis 2022 m. lapkričio-gruodžio mėn. atliktais testais „Protection", „Performance", „Usability" kategorijose.
7.	Administravimo konsolės aktyvavimas ir diegimas	Administravimo konsolė turi būti aktyvuojama gamintojo dedikuotoje paskyroje. Turi būti galimybė administravimo konsolę apsaugoti dviejų veiksnių autentifikacijos apsaugos sluoksniu. Turi būti galimybė administravimo konsolę diegti įmonės viduje. Tokiu atveju, gamintojas turi pateikti bent tris skirtingus administravimo konsolės diegimo formatus: - Viskas viename. - Įdiegimas pagal programos komponentus. - Virtuali mašina.
8.	Diegimo metodai	Kompiuterinėms darbo vietoms turi būti galimybės:

		- Įdiegti programinę įrangą centralizuotai iš valdymo konsolės. - Įdiegti programinę įrangą lokaliai iš diegimo laikmenos. - Įdiegti programinę įrangą per *Active Directory Group Policy* nustatymus.
9.	Būtini kompiuterinių darbo vietų apsaugos funkciniai moduliai	Antiviruso modulis – programinė įranga, sauganti nuo virusų, šnipinėjimo programų, grėsmių. Įsilaužimų prevencijos modulis (HIPS). Išorinių laikmenų apsaugos modulis. Galimybė atstatyti užkrėstą kompiuterį į ankstesnę būseną. Įsilaužimų blokatorius. Skydas nuo išpirkos reikalaujančių kenkėjų. Ugniasienė. Saugios naršyklės modulis. Sprendimas turi leisti pasirinkti, kuriuos apsaugos modulius aktyvuoti.
10.	Funkciniai reikalavimai kompiuterinių darbo vietų antiviruso moduliui	Antiviruso modulis – programinė įranga, sauganti nuo virusų, šnipinėjimo programų; Sprendime turi turėti tokias nuskaitymo parinktis: - Išmanusis nuskaitymas. - Kontekstinio meniu nuskaitymas. - Giluminis nuskaitymas. - Prie kompiuterio prijungtų išorinių laikmenų nuskaitymas (pvz. CD/DVD/USB). Galimybė vykdyti euristinį (angl. *heuristic*) nežinomų failų skenavimą. Galimybė slaptažodžiu apsaugoti nuo antivirusinės programinės įrangos nustatymų pakeitimo bei išdiegimo. Ugniasienės modulis – programinė įranga, sauganti nuo įsilaužimų. Apsaugos nuo elektroninių šiukšlių modulis (*Anti-SPAM*). Apsaugos nuo botnet tinklų modulis. Turi būti galimybė valdyti šiuos įrenginius: disko atminties įrenginius, CD/DVD, USB spausdintuvus, *FireWire* saugyklas, *Bluetooth* įrenginius, lustinių kortelių skaitytuvus, vaizdavimo įrenginius, modemus, LPT/COM prievadus, nešiojamuosius įrenginius. Sprendimas turi leisti/neleisti naudoti įrenginius pagal šiuos kriterijus: tiekėjas, modelis, serijinis numeris. Saugojimo įrenginiams sprendimas turi leisti nustatyti šiuos naudojimo leidimus: skaityti/rašyti, blokuoti, tik skaityti, įspėti.

		Įsilaužimų prevencijos modulis (HIPS) turi turėti šiuos režimus: automatinis, išsamusis, interaktyvusis, politika pagrįstas, mokymosi. Galimybė riboti prieigą prie internetinių šaltinių pagal adresą arba kategorijas. Turi būti integruota saugi naršyklė. Turi būti WMI ir viso registro nuskaitymas. Turi būti galimybė grafinę vartotojo sąsają pasirinkti lietuvių kalba. Kompiuterinių darbo vietų antivirusinės programos dokumentacija turi būti pateikta lietuvių kalba.
11.	Funkciniai reikalavimai darbo vietų ugniasienei	Turi apsaugoti nuo nepageidaujamų tinklo išorinių atakų, pagal nustatytus kriterijus (pagal prievadus (angl. *port*), programas) ribojant atakos šaltinio prieigą. Ugniasienė turi leisti/neleisti prisijungti, remiantis bet kuriuo iš šių režimų: automatinis, interaktyvus, politika pagrįstas, mokymosi. Darbo vietų ugniasienės valdymas turi būti atliekamas centralizuotai administravimo konsolės pagalba.
12.	Funkciniai reikalavimai mobiliųjų telefonų ir planšetinių kompiuterių antiviruso moduliui	Turi užtikrinti apsaugą nuo virusų ir kitų kenkėjiškų programų. Turi turėti galimybę skenuoti tiek vidinę, tiek išorinę (*micro SD* kortelių) įrenginio atmintį. Skenuoti tam tikrus nustatytus aplankus. Praradus įrenginį, turi būti galimybė nuotoliniu būdu gauti įrenginio buvimo koordinates, užrakinti ir apsaugoti nuo galimybės nesankcionuotai naudotis įrenginiu, saugiai ištrinti kontaktus, žinutes ir duomenis išorinėje laikmenoje (*micro SD*). Turi būti galimybė apsaugoti įrenginį sukčiavimo atveju. Turi būti galimybė nuotoliniu būdu įrenginyje paleisti sireną. Turi turėti apsaugos modulį nuo brukalų, leidžiantį apsaugoti įrenginį nuo nepageidaujamų skambučių ar SMS/MMS žinučių. Turi būti galimybė slaptažodžiu apsaugoti nuo antivirusinės programinės įrangos nustatymų pakeitimo bei išdiegimo.
13.	Funkciniai reikalavimai mobiliųjų įrenginių valdymo moduliui	Turi palaikyti centralizuotą administravimą nuotoliniu būdu. Valdymas turi būti įgyvendintas kuriant politikas, kurias galima priskirti įrenginiams ar įrenginių grupėms. Turi būti įgyvendinta galimybė užblokuoti mobiliąsias programėles arba jų kategorijas. Galimybė riboti programų naujinimąsi. Turi turėti galimybę uždrausti atstatyti įrenginio gamyklinius parametrus.

		Turi turėti galimybę uždrausti keisti įrenginio sisteminius parametrus. Turi turėti galimybę uždrausti pašalinti tam tikras mobiliąsias programėles. Turi turėti galimybę stebėti WI-FI, GPS, *Roaming* būklę. Turi turėti galimybę masiškai visiems telefonams siusti informacinį pranešimą tiesiai į ekraną. Turi turėti galimybę atvaizduoti įrenginyje sudiegtas mobiliąsias programėles ir jų versijas bei jas valdyti. Turi turėti galimybę užrakinti/atrakinti mobilųjį įrenginį per nuotolį be vartotojo pagalbos. Turi būti galimybė aktyvuoti patikimos SIM kortelės autentifikaciją. Turi būti galimybė įgalinti įrenginio šifravimą.
14.	Funkciniai reikalavimai valdymo konsolei	Turi palaikyti centralizuotą administravimą nuotoliniu būdu. Serveris turi bendrauti su galiniais įrenginiais per agentą, kuris gali saugoti politiką ir vykdyti užduotis, kol įrenginys yra neprisijungęs. Serveris turi leisti pridėti įrenginius prie valdymo konsolės naudojant šiuos metodus: - sinchronizavimas su *Active Directory*; - rankiniu būdu įvedus įrenginio vardą arba IP adresą; - technologija, gebanti aptikti įrenginius tinkle; Serveris turi leisti įdiegti saugumo sprendimus nuotoliniu būdu ir be vartotojo įsikišimo. Serveris turi leisti kurti statines ir dinamines grupes paprastesniam įrenginių administravimui. Serveris turi leisti nuotoliniu būdu vizualizuoti šią įrenginių informaciją: - pagrindinė informacija; - konfigūracija; - atliktos užduotys; - įdiegtos programos; - perspėjimai; - karantinas. Turi turėti centralizuotą bendros politikos (politikų) nustatymą visiems programinės įrangos klientams.

		Turi būti galimybė nustatyti automatinę produkto ir agento versijos atnaujinimo funkciją. Turi būti centralizuotai ir automatiškai atnaujinama klientų programinės dalies ir virusų parašų bazė, nereikalaujant sistemos įkrovimo iš naujo. Turi turėti funkcionalumą vartotojų grupėms nustatyti skirtingus klientinės dalies konfigūracinius nustatymus, taip kuriant pasirinktai grupei bendrą saugumo taisyklių rinkinį. Serveris turi turėti mobiliųjų įrenginių valdymo modulį, kuris leidžia prijungti ir valdyti mobiliuosius įrenginius. Turi turėti galimybę paveldėti taisykles (angl. *policies*) iš aukštesnio lygio nuotolinio administravimo serverio. Turi būti užtikrinta galimybė siųsti informacinius pranešimus į visų rūšių įrenginius, įskaitant stalinius kompiuterius, mobiliuosius įrenginius ar planšetinius kompiuterius. Serveris turi leisti apibrėžti aktyviklį, kuris įvykdytų numatytą veiksmą, kai tam tikras įvykis įvyksta tinkle. Pagal numatytuosius nustatymus serveris turi pateikti keletą standartinių ataskaitų bei leisti kurti naujus ataskaitų šablonus. Turi būti galimybė ataskaitas automatiškai gauti el. paštu arba generuoti valdymo konsolėje. Interneto konsolės sąsaja turi dirbti su informacijos skydais. Jie turi būti visiškai interaktyvūs ir leisti atlikti reikiamas užduotis iš kelių sekcijų. Turi būti realizuota galimybė keisti grafines naudotojo informacijos juostas realiuoju laiku. Turi būti galimybė prieigos profilius konfigūruoti naudojant skirtingus leidimus skirtingoms užduotims, pvz .: administratorius, ataskaitų kūrėjas, operatorius ir kita. Po 10 nesėkmingų bandymų prisijungti iš to paties IP adreso, serveris turi laikinai blokuoti tolesnius bandymus prisijungti iš šio IP adreso. Po 15 nesėkmingų bandymų vedant netinkamą seanso ID iš to paties IP adreso, serveris turi laikinai blokuoti tolesnius bandymus prisijungti iš šio IP adreso.
15.	Kiti reikalavimai	Sprendimas turi turėti mechanizmą, kuris leidžia pašalinti bet kurį kitą saugumo sprendimą, esantį galiniame įrenginyje. Šis mechanizmas turi būti: - Integruotas į saugumo sprendimą.

		- Pateiktas kaip atskiras įrankis. - Pasiekiamas per centralizuotą administravimo konsolę.
16.	Atnaujinimai	Klientinės dalies programinė įranga privalo turėti funkcionalumą parsisiųsti atnaujinimus tiesiai iš: - Gamintojo atnaujinimų serverio. - Centralizuoto valdymo serverio. Turi būti galimybė nustatyti automatinę saugumo produkto atnaujinimo funkciją.
17.	Aktualumo reikalavimas	Pateikiamoms licencijoms turi būti užtikrinamas gamintojo palaikymas sutarties galiojimo laikotarpiu, užtikrinantis teisę šiuo laikotarpiu be papildomo mokesčio operatyviai gauti naujausius virusų aprašus (angl. *signature*), virusų paieškos mechanizmo (angl. *engine*) atnaujinimus bei atsisiųsti ir diegtis naujausias programinės įrangos versijas.
18.	Versija	Turi būti siūloma naujausia stabili programinės įrangos versija, oficialiai gamintojo paskelbta internete.
19.	Dokumentacija	Turi būti pateikta aktuali dokumentacija, apimanti programinės įrangos įdiegimo, bendro naudojimo, administravimo, sistemos atstatymo procedūras.
20.	Gamintojo aptarnavimo (angl. *support*) sąlygos	Gamintojo atstovas turi teikti nemokamą pagalbą, konsultacijas telefonu, kreipiantis į pagalbos centrą darbo dienomis darbo valandomis lietuvių, rusų ir anglų kalbomis.
21.	Reikalavimai programinės įrangos naudojimo taisyklėms (licencijavimui)	Licencija turi suteikti teisę pakartotinai diegti siūlomą programinę įrangą neišnaudojant papildomos licencijos. Programinės įrangos licencijavimo taisyklėse licencija turi būti nepririšama prie aparatūrinės įrangos. Licencijos įsigijimo metu turi būti pateiktas vienas licencijos raktas, tinkantis visiems įrenginiams, nepriklausomai nuo licencijos įsigijimo kiekio bei įrenginio tipo.

2. .SPECIFIKACIJA KRITINIŲ DARBO VIETŲ IR TARNYBINIŲ STOČIŲ APSAUGAI

Eil. Nr.	Parametras	Minimali reikšmė
1.	Licencijų skaičius	200 vnt.

2.	Programinės įrangos tipas	Kompiuterinių darbo vietų, serverių, mobiliųjų ir planšetinių įrenginių apsauga nuo virusų ir šnipinėjimo programų, su ugniasiene ir el. pašto apsauga. Centralizuotas darbo vietų kietųjų diskų šifravimas. Papildoma apsauga nuo išpirkos reikalaujančių kenkėjų ir nulinės dienos atakų su debesyje valdoma smėliadėžės technologija. Papildoma *Microsoft 365* debesijos aplikacijų (*Exchange Online, OneDrive, Teams* ir *Sharepoint Online*) apsauga. Visi programinės įrangos sprendimai privalo būti valdomi iš vieno gamintojo administravimo konsolės debesijoje. Turi būti galimybė administravimo konsolę diegti organizacijos viduje.
3.	Programinės įrangos gamintojas	Turi būti nurodytas. Visi pateikti apsaugos nuo virusų, apsaugos nuo el. šiukšlių, kietųjų diskų šifravimo produktai, smėliadėžė debesyje ir Microsoft 365 debesijos aplikacijų apsauga turi būti pagaminti to paties gamintojo.
4.	Programinės įrangos paketo pavadinimas	Turi būti nurodytas.
5.	Palaikomos operacinės sistemos	Kompiuterinės darbo vietos: *Microsoft Windows 11 32-bitų ir 64-bitų.* *Microsoft Windows 10 32-bitų ir 64-bitų.* *macOS 10.12 ir naujesnės.* *Ubuntu Desktop 20.04 LTS.* *Ubuntu Desktop 22.04 LTS.* *Red Hat Enterprise Linux 7, 8 su įdiegta palaikoma darbalaukio aplinka.* *SUSE Linux Enterprise Desktop 15.* *Linux Mint 20.* Mobilieji įrenginiai: *Android 6 ir naujesnės.* *iOS 9 ir naujesnės.* *iPadOS 13 ir naujesnės.* Windows serveriai:

		Microsoft Windows Server 2022 (Server Core ir Desktop Experience). *Microsoft Windows Server 2019 (įskaitant Server Core, Desktop Experience ir Essentials).* *Microsoft Windows Server 2016 (įskaitant Server Core, Desktop Experience, Storage Server ir Essentials).* *Microsoft Windows Server 2012 R2 (įskaitant Storage Server ir Essentials).* *Server Core (Microsoft Windows Server 2012 R2).* Linux serveriai: *RedHat Enterprise Linux (RHEL) 7, 8 ir 9 versijos.* *CentOS 7 versijos.* *Ubuntu Server 20.04 LTS ir 22.04 LTS versijos.* *Debian 10 ir 11 versijos.* *SUSE Linux Enterprise Server (SLES) 12 ir 15 versijos.* *Oracle Linux 8 versijos.* *Amazon Linux 2 versijos.* Turi būti palaikomos virtualios aplinkos: *Microsoft Hyper-V Server 2012 ir naujesnė.* *VMware vSphere/ESXi 6.5 ir naujesnė.* *VMware Workstation 9 ir naujesnė.* *VMware Player 7 ir naujesnė.* *Oracle VirtualBox 6.0 ir naujesnė.* *Citrix 7.0 ir naujesnė.* Sprendimas su VMware ESXi turi palaikyti VMware Horizon 7.x ir 8.0 versijas. Nuotolinio administravimo konsolė saugumo sprendimams turi palaikyti (diegiant organizacijos viduje): *Microsoft Windows Server 2012 R2 64-bitų.* *Microsoft Windows Server 2012 R2 Core 64-bitų.*

		Microsoft Windows Storage Server 2012 R2 64-bitų. *Microsoft Windows Server 2016 64-bitų.* *Microsoft Windows Storage Server 2016 64-bitų.* *Microsoft Windows Server 2019 64-bitų.* *Microsoft Windows Server 2022 64-bitų.* *Linux: RHEL, Debian, Ubuntu, SLED, SLES, OpenSUSE, Fedora ir CentOS bei dauguma kitų RPM ir DEB paketų valdymu pagrįstų platinamų programų.* Nuotolinė saugumo sprendimų administravimo konsolė turi būti suderinama su naršyklėmis: • *Mozilla Firefox* • *Microsoft Edge* • *Google Chrome* • *Opera* • *Safari*
6.	Veikimo kokybės reikalavimai	Programinės įrangos gamintojas turi turėti ISO 9001:2015 ir ISO 27001:2013 arba lygiaverčius standartus atitinkančias sertifikacijas. Siūlomo produkto gamintojas turi būti *Leaders* arba *Challengers* kategorijose 2022 metų "Gartner Magic Quadrant for Endpoint Protection Platforms". Gamintojas turi būti įvertintas „TOP Player" įvertinimu 2023 metų "Radicati Endpoint Security Market Quadrant" rinkos tyrime. „AV-TEST" verslo produktų apžvalgos ir sertifikavimo ataskaitoje gamintojo saugumo sprendimai, skirti „Windows", turi būti įvertinti „TOP Product" įvertinimu, remiantis 2022 m. lapkričio-gruodžio mėn. atliktais testais „Protection", „Performance", „Usability" kategorijose.
7.	Administravimo konsolės aktyvavimas ir diegimas	Administravimo konsolė turi būti aktyvuojama gamintojo dedikuotoje paskyroje. Turi būti galimybė administravimo konsolę apsaugoti dviejų veiksnių autentifikacijos (angl. *Two Factor Authentication*) apsaugos sluoksniu.

		Turi būti galimybė administravimo konsolę diegti įmonės viduje. Tokiu atveju, gamintojas turi pateikti bent tris skirtingus administravimo konsolės diegimo formatus: - Viskas viename. - Įdiegimas pagal programos komponentus. - Virtuali mašina.
8.	Diegimo metodai	Kompiuterinėms darbo vietoms turi būti galimybės: - Įdiegti programinę įrangą centralizuotai iš valdymo konsolės. - Įdiegti programinę įrangą lokaliai iš diegimo laikmenos. - Įdiegti programinę įrangą per *Active Directory Group Policy* nustatymus. Microsoft 365 debesijos aplikacijų apsauga turi būti suderinama: - su Administratoriaus prieiga prie Azure Active Directory. - su prieiga prie Azure Cloud Services – Exchange (*mail*) | OneDrive. - su Microsoft 365, Exchange Online ir OneDrive prenumeratos planais: Microsoft 365 Education planai: ● Microsoft 365 A3 ● Microsoft 365 A5 Exchange Online planai: ● Exchange Online (Plan 1) ● Exchange Online (Plan 2) ● Microsoft 365 Business Standard OneDrive planai: ● OneDrive for Business (Plan 1) ● OneDrive for Business (Plan 2) ● Microsoft 365 Business Basic ● Microsoft 365 Business Standard

9.	Būtini kompiuterinių darbo vietų apsaugos funkciniai moduliai	Antiviruso modulis – programinė įranga, sauganti nuo virusų, šnipinėjimo programų, grėsmių. Įsilaužimų prevencijos modulis (HIPS). Išorinių laikmenų apsaugos modulis. Galimybė atstatyti užkrėstą kompiuterį į ankstesnę būseną. Įsilaužimų blokatorius. Skydas nuo išpirkos reikalaujančių kenkėjų. Ugniasienė. Kietųjų diskų šifravimo modulis. Saugios naršyklės modulis. Sprendimas turi leisti pasirinkti, kuriuos apsaugos modulius aktyvuoti.
10.	Funkciniai reikalavimai kompiuterinių darbo vietų antiviruso moduliui	Antiviruso modulis – programinė įranga, sauganti nuo virusų, šnipinėjimo programų; Sprendime turi turėti tokias nuskaitymo parinktis: - Išmanusis nuskaitymas. - Kontekstinio meniu nuskaitymas. - Giluminis nuskaitymas. - Prie kompiuterio prijungtų išorinių laikmenų nuskaitymas (pvz. CD/DVD/USB). Galimybė vykdyti euristinį (angl. *heuristic*) nežinomų failų skenavimą. Galimybė slaptažodžiu apsaugoti nuo antivirusinės programinės įrangos nustatymų pakeitimo bei išdiegimo. Ugniasienės modulis – programinė įranga, sauganti nuo įsilaužimų. Apsaugos nuo elektroninių šiukšlių modulis (*Anti-SPAM*). Apsaugos nuo botnet tinklų modulis. Turi būti galimybė valdyti šiuos įrenginius: disko atminties įrenginius, CD/DVD, USB spausdintuvus, FireWire saugyklas, Bluetooth įrenginius, lustinių kortelių skaitytuvus, skenavimo įrenginius, modemus, LPT/COM prievadus, nešiojamuosius įrenginius. Sprendimas turi leisti/neleisti naudoti įrenginius pagal šiuos kriterijus: tiekėjas, modelis, serijinis numeris.

		Saugojimo įrenginiams sprendimas turi leisti nustatyti šiuos naudojimo leidimus: skaityti/rašyti, blokuoti, tik skaityti, įspėti. Įsilaužimų prevencijos modulis (HIPS) turi turėti šiuos režimus: automatinis, išsamusis, interaktyvusis, politika pagrįstas, mokymosi. Galimybė riboti prieigą prie internetinių šaltinių pagal adresą arba kategorijas. Turi būti integruota saugi naršyklė. Turi būti WMI ir viso registro nuskaitymas. Turi būti galimybė grafinę vartotojo sąsają pasirinkti lietuvių kalba. Kompiuterinių darbo vietų antivirusinės programos dokumentacija turi būti pateikta lietuvių kalba.
11.	Funkciniai reikalavimai darbo vietų ugniasienei	Turi apsaugoti nuo nepageidaujamų tinklo išorinių atakų pagal nustatytus kriterijus (pagal prievadus (*port*), programas) ribojant atakos šaltinio prieigą. Ugniasienė turi leisti/neleisti prisijungti, remiantis bet kuriuo iš šių režimų: automatinis, interaktyvus, politika pagrįstas, mokymosi. Darbo vietų ugniasienės valdymas turi būti atliekamas centralizuotai administravimo konsolės pagalba.
12.	Funkciniai reikalavimai mobiliųjų telefonų ir planšetinių kompiuterių antiviruso moduliui	Turi užtikrinti apsaugą nuo virusų ir kitų kenkėjiškų programų. Turi turėti galimybę skenuoti tiek vidinę, tiek išorinę (*micro SD* kortelių) įrenginio atmintį. Skenuoti tam tikrus nustatytus aplankus. Praradus įrenginį, turi būti galimybė nuotoliniu būdu gauti įrenginio buvimo koordinates, užrakinti ir apsaugoti nuo galimybės nesankcionuotai naudotis įrenginiu, saugiai ištrinti kontaktus, žinutes ir duomenis išorinėje laikmenoje (*micro SD*). Turi būti galimybė apsaugoti įrenginį sukčiavimo atveju. Turi būti galimybė nuotoliniu būdu įrenginyje paleisti sireną. Turi turėti apsaugos modulį nuo brukalų, leidžiantį apsaugoti įrenginį nuo nepageidaujamų skambučių ar *SMS/MMS* žinučių. Turi būti galimybė slaptažodžiu apsaugoti nuo antivirusinės programinės įrangos nustatymų pakeitimo bei išdiegimo.

13.	Funkciniai reikalavimai pašto serveriui	Turi būti antiviruso modulis – programinė įranga, sauganti nuo virusų, šnipinėjimo programų. Turi būti *Antispam* komponentas - saugantis nuo el. šiukšlių. Turi būti *Anti-phishing* modulis - filtruojantis netinkamą turinį ir apsaugantis nuo asmens duomenų vagystės. Turi būti galimybė realiu laiku skenuoti visus prisegtus archyvus ir atlikti neutralizavimo veiksmus žinomų formatų byloms. Turi būti galimybė automatiškai skenuoti *POP3, IMAP, MAPI* ir *HTTP* protokolus nuo kenkėjiško turinio. Programinė įranga turi turėti galimybę sustabdyti/pratęsti skenavimą. Turi būti rezidentinės euristinės bei veiksmų analizės galimybės. Programinė įranga turi turėti keletą pasirinkimų, ką daryti su aptikta prisegta byla (neutralizuoti, ištrinti, talpinti į karantiną). Programinė įranga turi turėti apsaugą nuo el. šiukšlių, paremtą gamintojo surinkta duomenų baze apie brukalų siuntėjus, baltaisiais, juodaisiais ir pilkaisiais sąrašais. Turi būti galimybė administratoriui nurodyti specialią direktoriją, į kurią būtų siunčiami visi infekuoti laiškai. Turi būti užtikrinta integracija su *Active Directory*. Turi būti galimybė keisti apsaugos nuo el. šiukšlių nustatymus, taip pat galimybė vykdyti įvairias užduotis (antiviruso aprašų duomenų bazės atnaujinimą, antivirusinės programinės įrangos konfigūracijos modifikavimą pašto serveryje) iš centralizuoto valdymo įrankio. Turi būti galimybė eksportuoti valdymo konsolės nustatymus ir juos panaudoti pakartotinio diegimo metu. Galimybė matyti detalias sistemos būklės ataskaitas valdymo konsolėje. Turi būti pateikti tokie duomenys: paskutinio atnaujinimo laikas ir rezultatas, virusų aprašų kiekis, skenavimo variklio versija ir aktyvūs programos moduliai. Turi būti galimybė gauti detalias ataskaitas apie skenavimo veiksmus. Turi būti galimybė administratoriui el. paštu gauti pranešimus apie sistemos įvykius: aptikus netinkamus laiškus, aptiktus kenkėjiškus archyvus ar atakas.

		Turi būti galimybė automatiškai atnaujinti antivirusų aprašų duomenų bazę tiesiogiai iš interneto arba centralizuotu būdu, siekiant išvengti per didelės tinklo apkrovos bei tinklo sutrikimų. Turi būti galimybė nustatyti atnaujinimų vietą, internetu naudojant *proxy* (su vartotojo vardu ir slaptažodžiu). Turi būti galimybė atlikti Office 365 pašto dėžutės nuskaitymą. Turi turėti funkciją nesiųsti atmetimo žinutės laiško siuntėjui (angl. *Backscatter protection*). Turi būti galimybė siųsti el. pašto karantino ataskaitas nurodytiems vartotojams ir administratoriams. Turi turėti galimybę sinchronizuoti informaciją ir konfigūraciją tarp administravimo konsolės ir pašto serverio(-ių). Turi turėti galimybę integruotis su trečiųjų šalių nuotolinio stebėjimo ir valdymo programine įranga (*RMM*). Turi būti galimybė eksportuoti žurnalo įrašus į *syslog* serverį, kurie galėtų būti panaudojami su kitomis saugumo informacijos ir įvykių valdymo sistemomis (*SIEM*) ir žurnalų valdymo sprendimais. Turi turėti funkciją blokuoti pašto serverio tinklo ryšį. Turi turėti mašininiu mokymusi paremtą apsaugą - gebėti skenuoti failus, paštą ir tinklo srautą. Turi turėti apsaugą nuo sukčiavimo apsimetant kitu laiško siuntėju (angl. *spoofing*).
14.	Funkciniai reikalavimai Microsoft 365 debesijos aplikacijų apsaugai	Turi būti antiviruso modulis (angl. *Anti-Malware*) – programinė įranga, gebanti saugotis nuo virusų, šnipinėjimo programų ir kitų kenkėjiškų failų bei grėsmių. Turi būti galimybė realiu laiku skenuoti visus prisegtus archyvus ir atlikti neutralizavimo veiksmus žinomų formatų byloms. Turi būti galimybė automatiškai skenuoti *POP3, IMAP, MAPI ir HTTP* protokolus nuo kenkėjiško turinio. Programinė įranga turi turėti galimybę sustabdyti/pratęsti skenavimą/apsaugą. Turi būti galimybė aktyvuoti rezidentinės euristinės analizės funkciją.

		Programinė įranga turi turėti keletą pasirinkimų, kaip elgtis su aptiktu kenkėjišku prisegtu failu (pvz., neutralizuoti, ištrinti, talpinti į karantiną). Programinė įranga turi turėti apsaugą nuo el. šiukšlių, paremtą gamintojo surinkta duomenų baze apie brukalų siuntėjus, baltaisiais, juodaisiais ir pilkaisiais sąrašais. Turi būti galimybė administratoriui nurodyti specialią pašto direktoriją, į kurią bus siunčiami visi infekuoti laiškai. Turi būti galimybė keisti, apsaugos nuo el. šiukšlių, kenkėjiškų failų nustatymus, taip pat turėti papildomus nustatymus skirtus apsaugoti *Microsoft OneDrive, Teams* ir *Sharepoint site*s aplinką iš centralizuoto valdymo puslapio. Turi būti galimybė matyti detalias sistemos apsaugos būklės ataskaitas valdymo konsolėje. Turi būti galimybė administratoriui el. paštu gauti pranešimus apie sistemos įvykius: aptikus netinkamus laiškus, aptiktus kenkėjiškus archyvus ar atakas. Turi būti galimybė aktyvuoti mašininio mokymosi apsaugą. Turi būti *Exchange Online, OneDrive, Teams* ir *Sharepoint sites* karantino tvarkyklė su galimybe peržiūrėti karantine esančius objektus ir atlikti atitinkamą veiksmą (atsisiųsti, ištrinti arba paleisti). Turi būti saugumo politikos su galimybe turėti kelis saugumo skyrius ir konfigūruoti skirtingus kiekvieno organizacinio vieneto apsaugos nustatymus. Turi turėti galimybę sukonfigūruotą politiką su apsaugos nustatymais priskirti pasirinktiems tenantams (angl. *tenant*), vartotojams ar vartotojų grupėms. Turi būti *Multi-tenant* palaikymas - vienoje valdymo konsolėje galimybė apsaugoti ir valdyti kelis Office 365 tenantus.
15.	Funkciniai reikalavimai smėliadėžės debesyje paslaugai	Galiniuose įrenginiuose turi būti aktyvuojama nuotoliniu būdu naudojant administravimo konsolę. Turi būti galimybė įtartinus failus į smėliadėžę debesyje teikti tiek rankiniu, tiek automatiniu būdu.

		Visi į smėliadėžę išsiųsti failai turi būti fiksuojami nuotolinio administravimo konsolėje. Turi būti galimybė gauti ataskaitas apie išsiųstus įtartinus failus. Turi būti galimybė nustatyti terminą, kiek dienų gali būti saugomi įtartini failai smėliadėžėje. Turi būti galimybė drausti/leisti dokumentų siuntimą į smėliadėžę.
16.	Funkciniai reikalavimai mobiliųjų įrenginių valdymo moduliui	Turi palaikyti centralizuotą administravimą nuotoliniu būdu. Valdymas įgyvendinamas kuriant politikas, kurios vėliau priskiriamos įrenginiams ar įrenginių grupėms. Turi būti įgyvendinta galimybė užblokuoti mobiliąsias programėles arba jų kategorijas. Galimybė riboti programų naujinimąsi. Turi turėti galimybę uždrausti atstatyti įrenginio gamyklinius parametrus. Turi turėti galimybę uždrausti keisti įrenginio sisteminius parametrus. Turi turėti galimybę uždrausti pašalinti tam tikras mobiliąsias programėles. Turi turėti galimybę stebėti *WI-FI, GPS, Roaming* būklę. Turi turėti galimybę masiškai visiems telefonams siusti informacinį pranešimą tiesiai į ekraną. Turi turėti galimybę atvaizduoti įrenginyje sudiegtas mobiliąsias programėles ir jų versijas bei jas valdyti. Turi turėti galimybę užrakinti/atrakinti mobilųjį įrenginį per nuotolį be vartotojo pagalbos. Turi būti galimybė aktyvuoti patikimos SIM kortelės autentifikaciją. Turi būti galimybė įgalinti įrenginio šifravimą.
17.	Funkciniai reikalavimai darbo vietų šifravimo moduliui	Turi palaikyti centralizuotą administravimą nuotoliniu būdu. Valdymas turi būti įgyvendintas kuriant politikas, kurias galima priskirti įrenginiams ar įrenginių grupėms.

		Turi būti suderinamumas su *Microsoft Windows 10* / 11 operacinėmis sistemomis. Turi būti UEFI mikroprogramos (angl. *firmware*) palaikymas. Turi būti TPM (angl. *Trusted Platform Module*) palaikymas Turi būti OPAL diskų palaikymas. Turi turėti galimybę šifruoti visus diskus arba tik krovimosi diską. Turi turėti galimybę centralizuotai nustatyti šifravimo slaptažodžio politiką. Turi būti galimybė centralizuotai politikoje laikinai atjungti šifravimo slaptažodžio reikalavimą. Turi turėti galimybę administratoriui nuotoliniu būdu inicijuoti šifravimo slaptažodžio atkūrimą, blokavimą ir ištrynimą. Turi būti galimybė administratoriui iššifruoti kietąjį diską su gamintojo numatyta atkūrimo programa.
18.	Funkciniai reikalavimai valdymo konsolei	Turi palaikyti centralizuotą administravimą nuotoliniu būdu. Serveris turi bendrauti su galutiniais įrenginiais per agentą, kuris gali saugoti politiką ir vykdyti užduotis, kol įrenginys yra neprisijungęs. Serveris turi leisti pridėti įrenginius prie valdymo konsolės naudojant šiuos metodus: - sinchronizavimas su *Active Directory*; - rankiniu būdu įvedus įrenginio vardą arba IP adresą; - technologija, gebanti aptikti įrenginius tinkle; Serveris turi leisti įdiegti saugumo sprendimus nuotoliniu būdu ir be vartotojo įsikišimo. Serveris turi leisti kurti statines ir dinamines grupes paprastesniam įrenginių administravimui. Serveris turi leisti nuotoliniu būdu vizualizuoti šią įrenginių informaciją: - pagrindinė informacija; - konfigūracija; - atliktos užduotys; - įdiegtos programos; - perspėjimai; - karantinas.

		Turi turėti centralizuotą bendros politikos (politikų) nustatymą visiems programinės įrangos klientams. Turi būti galimybė nustatyti automatinę produkto ir agento versijos atnaujinimo funkciją. Turi būti centralizuotai ir automatiškai atnaujinama klientų programinės dalies ir virusų parašų bazė, nereikalaujant sistemos įkrovimo iš naujo. Turi turėti funkcionalumą vartotojų grupėms nustatyti skirtingus klientinės dalies konfigūracinius nustatymus, taip kuriant pasirinktai grupei bendrą saugumo taisyklių rinkinį. Serveris turi turėti mobiliųjų įrenginių valdymo modulį, kuris leidžia prijungti ir valdyti mobiliuosius įrenginius. Turi turėti galimybę paveldėti taisykles (angl. *policies*) iš aukštesnio lygio nuotolinio administravimo serverio. Turi būti užtikrinta galimybė siųsti informacinius pranešimus į visų rūšių įrenginius, įskaitant stalinius kompiuterius, mobiliuosius įrenginius ar planšetinius kompiuterius. Serveris turi leisti apibrėžti aktyviklį, kuris įvykdytų numatytą veiksmą, kai tam tikras įvykis įvyksta tinkle. Pagal numatytuosius nustatymus serveris turi pateikti keletą standartinių ataskaitų bei leisti kurti naujus ataskaitų šablonus. Turi būti galimybė ataskaitas automatiškai gauti el. paštu arba generuoti valdymo konsolėje. Interneto konsolės sąsaja turi dirbti su informacijos skydais. Jie turi būti visiškai interaktyvūs ir leisti atlikti reikiamas užduotis iš kelių sekcijų. Turi būti realizuota galimybė keisti grafines naudotojo informacijos juostas realiuoju laiku. Turi būti galimybė prieigos profilius konfigūruoti naudojant skirtingus leidimus skirtingoms užduotims, pvz .: administratorius, ataskaitų kūrėjas, operatorius ir kita. Po 10 nesėkmingų bandymų prisijungti iš to paties IP adreso, serveris turi laikinai blokuoti tolesnius bandymus prisijungti iš šio IP adreso. Po 15 nesėkmingų bandymų vedant netinkamą seanso ID iš to paties IP adreso, serveris turi laikinai blokuoti tolesnius bandymus prisijungti iš šio IP adreso.

19.	Funkciniai reikalavimai valdymo konsolės Microsoft 365 debesijos aplikacijų apsaugos moduliui	Turi palaikyti centralizuotą administravimą nuotoliniu būdu. Serveris turi leisti įjungti saugumo sprendimus nuotoliniu būdu ir be vartotojo įsikišimo. Turi būti galimybė ataskaitas automatiškai gauti el. paštu arba generuoti valdymo konsolėje. Serveris turi leisti sinchronizuoti statines grupes iš Microsoft Office 365 į apsaugos sprendimo valdymo konsolę paprastesniam vartotojų administravimui. Serveris turi leisti nuotoliniu būdu vizualizuoti šią vartotojų informaciją: - pagrindinė informacija; - konfigūracija; - karantinas. Turi turėti centralizuotą bendrųjų politikų (*policies*) priskyrimą visiems klientams/paskyroms. Turi būti centralizuotai ir automatiškai atnaujinama klientų dalies ir virusų parašų bazė, nereikalaujant sistemos įkrovimo iš naujo. Turi turėti galimybę paveldėti taisykles (*policies*) iš aukštesnio lygio. Pagal numatytuosius nustatymus serveris turi pateikti keletą standartinių ataskaitų bei leisti kurti naujus ataskaitų šablonus. Interneto konsolės sąsaja turi dirbti su informacijos skydais. Jie turi būti visiškai interaktyvūs ir leisti atlikti reikiamas užduotis iš kelių sekcijų.
20.	Kiti reikalavimai	Sprendimas turi turėti mechanizmą, kuris leidžia pašalinti bet kurį kitą saugumo sprendimą, esantį galiniame įrenginyje. Šis mechanizmas turi būti: - Integruotas į saugumo sprendimą. - Pateiktas kaip atskiras įrankis. - Pasiekiamas per centralizuotą administravimo konsolę.
21.	Atnaujinimai	Klientinės dalies programinė įranga privalo turėti funkcionalumą parsisiųsti atnaujinimus tiesiai iš: - Gamintojo atnaujinimų serverio. - Centralizuoto valdymo serverio.

22.	Aktualumo reikalavimas	Pateikiamoms licencijoms turi būti užtikrinamas gamintojo palaikymas sutarties galiojimo laikotarpiu, užtikrinantis teisę šiuo laikotarpiu be papildomo mokesčio operatyviai gauti naujausius virusų aprašus (angl. *signature*), virusų paieškos mechanizmo (angl. *engine*) atnaujinimus bei atsisiųsti ir diegtis naujausias programinės įrangos versijas.
23.	Versija	Turi būti siūloma naujausia stabili programinės įrangos versija, oficialiai gamintojo paskelbta internete.
24.	Dokumentacija	Turi būti pateikta aktuali dokumentacija, apimanti programinės įrangos įdiegimo, bendro naudojimo, administravimo, sistemos atstatymo procedūras.
25.	Gamintojo aptarnavimo (angl. support) sąlygos	Gamintojo atstovas turi teikti nemokamą pagalbą, konsultacijas telefonu, kreipiantis į pagalbos centrą darbo dienomis darbo valandomis lietuvių, rusų ir anglų kalbomis.
26.	Reikalavimai programinės įrangos naudojimo taisyklėms (licencijavimui)	Licencija turi suteikti teisę pakartotinai diegti siūlomą programinę įrangą neišnaudojant papildomos licencijos. Programinės įrangos licencijavimo taisyklėse licencija turi būti nepririšama prie aparatūrinės įrangos arba vartotojo paskyros. Licencijos įsigijimo metu turi būti pateiktas vienas licencijos raktas, tinkantis visiems įrenginiams, nepriklausomai nuo licencijos įsigijimo kiekio bei įrenginio tipo.

UAB „NBCS
Uždaroji akcinė bendrovė, Šeškinės sodų g. 12, LT-08343 Vilnius, Lietuva, Tel.: +370 5 2764563, Lietuvos Respublikos juridinių asmenų registras, Įm. kodas: 301817848, PVM mok. kodas: LT100006470618

Lietuvos nacionalinei Martyno Mažvydo bibliotekai
Gedimino pr. 51, 01109 Vilnius

PASIŪLYMAS
ANTIVIRUSINIŲ PROGRAMŲ TIPINĖMS IR KRITINĖMS DARBO VIETOMS PIRKIMUI
2023-10-06
(Data)
Vilnius
(Vieta)

1. INFORMACIJA APIE TIEKĖJĄ

Tiekėjo pavadinimas / Tiekėjų grupės narių pavadinimai	UAB „NBCS“
Tiekėjų grupės bendras atstovas arba vadovaujantis narys *(pildoma, jei Pasiūlymą teikia Tiekėjų grupė)*	
Tiekėjo adresas(-ai)[1] *(jei skiriasi, taip pat nurodyti ir adresą korespondencijai)*	Šeškinės sodų g. 12, LT-08343 Vilnius
Tiekėjo arba tiekėjų grupės narių juridinio asmens kodas (-ai) *(tuo atveju, jei Pasiūlymą teikia fizinis asmuo - verslo pažymėjimo Nr. ar pan.)*	301817848
Pasiūlymo pasirašymui Tiekėjo / Tiekėjų grupės bendro atstovo arba vadovaujančio nario įgalioto asmens vardas, pavardė, pareigos	[redacted]
Pasiūlymą pateikusio Tiekėjo / Tiekėjų grupės bendro atstovo arba vadovaujančio nario kontaktinio asmens telefono numeris / Mobilaus telefono numeris ir el. paštas	[redacted]3485,

Informacija apie kiekvieno **Tiekėjų grupės** nario savo jėgomis numatomų tiekti prekių / teikti paslaugų / atlikti darbų dalį (*pildoma, kai Pasiūlymą pateikia Tiekėjų grupė*)

Eil. Nr.	Tiekėjų grupės nario pavadinimas	Numatoma tiekti prekių / teikti paslaugų / atlikti darbų dalis
1.		
...		

2. INFORMACIJA APIE PASIŪLYMĄ PATEIKUSIO TIEKĖJO / JUNGTINĖS VEIKLOS ATSAKINGOJO PARTNERIO (KONTAKTINĮ) ASMENĮ

Vardas, Pavardė	[redacted]
Telefono numeris / Mobilaus telefono numeris	
Elektroninio pašto adresas	

[1] Tuo atveju, jei Pasiūlymą teikia Jungtinei veiklai susivienijusių Tiekėjų grupė, pateikiama informacija apie visus jungtinei veiklai susivienijusius Tiekėjus.

3. SUTIKIMAS SU PIRKIMO SĄLYGOMIS

Pažymime, kad pateikdami savo Pasiūlymą, sutinkame su visomis Pirkimo sąlygomis (įskaitant priedus), kitais Pirkimo dokumentais (jų paaiškinimas, papildymais) ir tolesnėmis Pirkimo procedūromis ir būsimos Sutarties sąlygomis (jei pridėtas sutarties projektas).

Patvirtiname, kad atidžiai perskaitėme visus Pirkimo sąlygų, tame tarpe ir Techninės specifikacijos, reikalavimus, mūsų Pasiūlymas juos visiškai atitinka ir įsipareigojame jų laikytis vykdydami Sutartį. Taip pat įsipareigojame laikytis ir kitų Lietuvos Respublikoje galiojančių ir Pirkimo objektui bei Sutarčiai taikomų teisės aktų reikalavimų. Rengdami Pasiūlymą, atsižvelgėme į darbų saugos ir darbo sąlygų reikalavimus.

4. INFORMACIJA APIE PLANUOJAMUS PASITELKTI SUBTIEKĖJUS IR (AR) KITUS ŪKIO SUBJEKTUS

Sutarties vykdymui bus pasitelkiami šie **subtiekėjai**[2] ir jiems perduodama vykdyti sutarties dalis:

Eil. Nr.	Subtiekėjo pavadinimas[3], jei pasitelkiamas juridinis asmuo, arba vardas, pavardė, jei pasitelkiamas fizinis asmuo	Subtiekėjui perduodama vykdyti sutartinių įsipareigojimų dalis, kuriai nekeliami kvalifikacijos reikalavimai[4]

Kartu su Pasiūlymu pateikiamos Subtiekėjų užpildytas ir pasirašytas deklaracijas (jeigu jie yra žinomi).

Tretieji asmenys, kurių priemonėmis tiekėjas naudojasi (naudosis), tačiau kurie tiesiogiai aktyviai, savo veiksmais neprisidės prie perkančiosios organizacijos poreikio įsigyti pirkimo objektą tenkinimo *(tiesiogiai neteiks dalies paslaugų ar kitaip tiesiogiai nedalyvaus vykdant pirkimo sutartį)*:

Eil. Nr.	Trečiojo asmens, kurių priemonėmis tiekėjas naudojasi (naudosis), pavadinimas, jei pasitelkiamas juridinis asmuo, arba vardas, pavardė, jei pasitelkiamas fizinis asmuo	Trečiųjų asmenų perduodamos priemonės, vykdant sutartinius įsipareigojimus

5. PASIŪLYMO KAINA

Pasiūlymo kaina nurodoma eurais užpildant žemiau pateiktą lentelę:

Eil. Nr.	**Pirkimo objektas**	**Kiekis Sutarties galiojimo laikotarpiu**	**Programinės įrangos gamintojas**	**Programinės įrangos paketo pavadinimas**	**1 vnt. įkainis, EUR be PVM**	**Viso kaina, EUR be PVM[5]**
1.	Antivirusinės programos licencijos tipinėms darbo vietoms / tarnybinėms stotims	300 vnt.	ESET	ESET Protect Entry (Cloud)	16,00	4800,00
2.	Antivirusinės programos licencijos kritinėms darbo vietoms / tarnybinėms stotims	200 vnt.	ESET	ESET Protect Complete (Cloud)	25,00	5000,00
					Pasiūlymo kaina, EUR be PVM[6]:	9800,00
					PVM_____ *(21%)*:	2058,00
					Pasiūlymo kaina EUR su PVM:	11858,00

[2] Subtiekėjai, kurie bus pasitelkti vykdant Pirkimo sutartį ir kurių pajėgumais (kvalifikacija) nesiremiama.

[3] Nurodomas konkretus Subtiekėjo pavadinimas, jei žinomas Pasiūlymų pateikimo metu. Jei ketinama pasitelkti, tačiau konkretus pavadinimas nėra žinomas, nurodoma „Nežinomas“.

[4] Toks perdavimas nekeičia pagrindinio Tiekėjo atsakomybės dėl numatomos sudaryti Sutarties įvykdymo.

[5] Kaina, EUR be PVM apskaičiuojama padauginant įkainį, EUR be PVM iš kiekio Sutarties galiojimo laikotarpiu.

[6] Pasiūlymo kaina, EUR be PVM turi apimti visas išlaidas, visus mokesčius, išskyrus PVM mokestį, mokėtinus pagal galiojančius Lietuvos Respublikos įstatymus, įskaitant sąskaitų pateikimo kaštus per „E. sąskaita“ sistemą.

* Tais atvejais, kai pagal galiojančius teisės aktus Tiekėjui nereikia mokėti PVM, jis lentelių eilučių, kur nurodyta „PVM“ ir „Pasiūlymo kaina EUR su PVM“ – nepildo ir nurodo priežastis, dėl kurių PVM nemoka _____.

6. PASIŪLYMO GALIOJIMO TERMINAS

Pasiūlymas galioja 3 mėnesius nuo pasiūlymų pateikimo termino pabaigos.

7. KONFIDENCIALI INFORMACIJA

Prašome nurodyti, ar yra konfidencialios informacijos ir kokia nurodyta informacija yra konfidenciali. Tuo atveju, jei lentelė ar atskiros jos eilutės nėra užpildomos, Perkančioji organizacija laikys, kad ta Pasiūlymo informacija arba atitinkama jos dalis nėra laikoma konfidencialia. Konfidencialia negali būti laikoma informacija, kuri atitinka LR VPĮ 20 straipsnio 2 dalyje nustatytus požymius ir sąlygas.

Eil. Nr.	Dokumento pavadinimas[7]	Kokiu pagrindu atitinkamas dokumentas yra konfidencialus?
1.	V. Gricukės įgaliojimas_konfidencialu	Dėl asmens duomenų apsaugos
...		

Pasirašydamas šį Pasiūlymą, tvirtintu, kad:

1) Pasiūlymo dokumentuose pateikti duomenys yra tikri;
2) siūlomas Pirkimo objektas visiškai atitinka Pirkimo dokumentuose nustatytus reikalavimus.

_____

(Tiekėjo arba jo įgalioto asmens vardas, pavardė, parašas)[8]

PRIEDAI:

1. Priedas Nr. 1. V. Gricukės įgaliojimas_konfidencialu, 1 lapas.
2. Priedas Nr. 2. Nacionalinio saugumo reikalavimų atitikties deklaracija, 1 lapas.

[7] Atskiri dokumentai ar šiuose dokumentuose pateikiama informacija gali būti nurodoma atskirose eilutėse, atsižvelgiant į informacijos konfidencialumą. Sąrašas nėra baigtinis.

[8] Jei Pasiūlymą Pirkimui pasirašo vadovo įgaliotas asmuo, prie pasiūlymo turi būti pridėtas rašytinis įgaliojimas arba kitas dokumentas, suteikiantis parašo teisę.

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	
Dokumento pavadinimas (antraštė)	
Dokumento registracijos data ir numeris	
Dokumento gavimo data ir dokumento gavimo registracijos numeris	
Dokumento specifikacijos identifikavimo žymuo	
Parašo paskirtis	
Parašą sukūrusio asmens vardas, pavardė ir pareigos	
Sertifikatas išduotas	
Parašo sukūrimo data ir laikas	
Parašo formatas	
Laiko žymoje nurodytas laikas	
Informacija apie sertifikavimo paslaugų teikėją	
Sertifikato galiojimo laikas	
Parašo paskirtis	
Parašą sukūrusio asmens vardas, pavardė ir pareigos	
Sertifikatas išduotas	
Parašo sukūrimo data ir laikas	
Parašo formatas	
Laiko žymoje nurodytas laikas	
Informacija apie sertifikavimo paslaugų teikėją	
Sertifikato galiojimo laikas	
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	
Pagrindinio dokumento priedų skaičius	
Pagrindinio dokumento pridedamų dokumentų skaičius	
Pridedamo dokumento sudarytojas (-ai)	
Pridedamo dokumento pavadinimas (antraštė)	
Pridedamo dokumento registracijos data ir numeris	
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	
Paieškos nuoroda	
Papildomi metaduomenys	