PIRKIMO–PARDAVIMO SUTARTIS NR. _____

2025 m. kovo d.
Palanga

Palangos miesto savivaldybės administracija, juridinio asmens kodas 125196077, kurios registruota buveinė yra Vytauto g. 112, LT-00153 Palanga, duomenys apie įstaigą kaupiami ir saugomi Lietuvos Respublikos juridinių asmenų registre, atstovaujama administracijos direktorės Ramunės Olšauskaitės Urbonienės, veikiančios pagal Palangos miesto savivaldybės mero 2024 m. birželio 19 d. potvarkį Nr. M2-101 „Dėl Ramunės Olšauskaitės Urbonienės perkėlimo į Palangos miesto savivaldybės administracijos direktoriaus pareigas ir priemokos jai skyrimo“, (toliau – Pirkėjas) ir UAB „CSC Telecom“, juridinio asmens kodas 111818067, kurios registruota buveinė yra Perkūnkiemio g. 7, LT-12131 Vilnius, duomenys apie įmonę kaupiami ir saugomi Lietuvos Respublikos juridinių asmenų registre, atstovaujama pardavimų vadovo Tado Ivašausko, veikiančio pagal 2025 m. sausio mėn. 2 d. įgaliojimą Nr. CSC250102/02, (toliau – Pardavėjas), toliau kartu šioje prekių pirkimo–pardavimo sutartyje vadinami Šalimis, o kiekvienas atskirai – Šalimi, sudarė šią pirkimo–pardavimo sutartį, toliau vadinamą Sutartimi, ir susitarė dėl toliau išvardytų sąlygų.

I. SUTARTIES OBJEKTAS

1.1. Antivirusinės programinės įrangos *ESET Protect Elite cloud* 150 vnt. licencijų (toliau – Prekės), atitinkančių Sutarties 2 priede nustatytus reikalavimus, pirkimas–pardavimas.

II. SUTARTIES KAINA

2.1. Sutarties kaina, nustatyta neskelbiamos apklausos būdu, yra 15972,00 Eur (*penkiolika tūkstančių devyni šimtai septyniasdešimt du eurai 00 ct*).

III. SUTARTIES KAINODARA IR ATSISKAITYMAS

3.1. Sutarčiai taikomas fiksuotos kainos kainodara.

3.2. Į Prekių kainą įskaitytos visos išlaidos ir mokesčiai bei visos Sutarties įvykdymo išlaidos.

3.3. Vykdant Sutartį, PVM sąskaita faktūra turi būti teikiama naudojantis informacinės sistemos SABIS priemonėmis. Kiti išlaidas pagrindžiantys dokumentai gali būti teikiami naudojantis informacinės sistemos SABIS priemonėmis. Prisijungti prie elektroninės paslaugos SABIS galima interneto adresu https://sabis.nbfc.lt/. Paslauga yra apmokama Lietuvos Respublikos finansų ministro nustatyta tvarka. Pardavėjas įsipareigoja PVM sąskaitoje faktūroje nurodyti sutarties, kurios pagrindu išrašomos sąskaitos, numerį.

3.4. Visi atsiskaitymai vykdomi eurais, pavedimu į Sutartyje nurodytas Šalių atsiskaitomąsias banko sąskaitas. Pasikeitus banko sąskaitai, Šalis privalo informuoti apie šį pasikeitimą per protingą terminą, kuris negali būti ilgesnis kaip 7 (septynios) darbo dienos.

3.5. Sumokėjimo už Prekes diena yra laikoma diena, kai Pirkėjas atliko pavedimą iš savo banko sąskaitos į Sutartyje nurodytą Pardavėjo banko sąskaitą;

3.6. Prekių kaina dėl pasikeitusių mokesčių perskaičiuojama tokia tvarka:

3.6.1. mokestis, kuriam pasikeitus perskaičiuojama Prekių kaina: pridėtinės vertės mokestis (toliau – PVM). Pasikeitus kitiems mokesčiams Prekių kaina neperskaičiuojama;

3.6.2. perskaičiavimas atliekamas įsigaliojus Lietuvos Respublikos pridėtinės vertės mokesčio įstatymo pakeitimo įstatymui, kuriuo keičiasi mokesčio tarifas;

3.6.3. perskaičiavimo formulė: pasikeitus PVM tarifo dydžiui, Prekių kainoje esantis PVM tarifas negautoms Prekėms keičiamas (mažinamas ar didinamas) pagal Lietuvos Respublikos galiojančius teisės aktus;

3.6.4. Prekių kainos pakeitimas įforminamas atskiru Pardavėjo ir Pirkėjo pasirašytu susitarimu, kuriame užfiksuojama perskaičiuota Sutarties kaina;

3.6.5. perskaičiuota Prekių kaina pradedama taikyti nuo Pridėtinės vertės mokesčio įstatymo pakeitimo įstatymo, kuriuo keičiasi šio mokesčio tarifas, nurodytos tarifo įsigaliojimo dienos.

3.7. Bet kuri Sutarties šalis Sutarties galiojimo metu turi teisę inicijuoti Sutarties kainos peržiūrą (keitimą) ne anksčiau kaip po 6 (šešių) mėnesių nuo Sutarties įsigaliojimo dienos (jeigu peržiūra jau buvo atlikta – nuo Susitarimo dėl paskutinio perskaičiavimo pagal šį Specialiųjų sąlygų punktą įsigaliojimo dienos). Sutarties kainos peržiūra atliekama ne rečiau kaip kas 6 (šeši) mėnesiai.

3.8. Sutarties kaina peržiūrima tik tai Sutarties daliai, kuri nėra išpirkta, t. y., Prekėms, kurios nėra priimtos ir apmokėtos. Vėlesnė Sutarties kainos peržiūra negali apimti laikotarpio, už kurį jau buvo atliktas peržiūra.

3.9. Jeigu Prekių suteikimas vėluoja dėl Pardavėjo kaltės, uždelstų suteikti Prekių kaina nėra perskaičiuojama dėl kainų lygio kilimo (negali būti didinami).

3.10. Atlikdamos Sutarties kainos peržiūrą Šalys vadovaujasi Valstybės duomenų agentūros viešai Oficialiosios statistikos portale paskelbtais Rodiklių duomenų bazės duomenimis arba kitų oficialių šaltinių duomenimis. Iš kitos Šalies nereikalaujama pateikti oficialaus Valstybės duomenų agentūros ar kitos institucijos išduoto dokumento ar patvirtinimo.

3.11. Šalys privalo Susitarime nurodyti vartojimo prekių ir paslaugų indekso reikšmę laikotarpio pradžioje ir jo nustatymo datą, indekso reikšmę laikotarpio pabaigoje ir jo nustatymo datą, kainų pokytį (k), perskaičiuotą Sutarties kainą, perskaičiuotą Pradinės Sutarties vertę.

3.12. Nauja Sutarties kaina apskaičiuojama pagal žemiau pateiktą formulę:

$$a_1 = a + \left(\frac{k}{100} \times a\right)$$, kai

a – kaina (Eur be PVM)) (jei peržiūra jau buvo atlikta, tai po paskutinio perskaičiavimo);

a_1 – perskaičiuota (pakeista) kaina (Eur be PVM);

k – pagal vartotojų kainų indeksą (bendras indeksas) apskaičiuotas Vartojimo prekių ir paslaugų kainų pokytis (padidėjimas arba sumažėjimas) (proc.). „k“ reikšmė skaičiuojama pagal formulę:

$$k = \frac{Ind_{naujausias}}{Ind_{pradžia}} \times 100 - 100$$, (proc.) kai

$Ind_{naujausias}$ – kreipimosi dėl kainos peržiūros išsiuntimo kitai šaliai dieną paskelbtas naujausias vartojimo prekių ir paslaugų indeksas („Vartojimo prekių ir paslaugų“);

$Ind_{pradžia}$ – laikotarpio pradžios datos (mėnesio) vartojimo prekių ir paslaugų indeksas („Vartojimo prekių ir paslaugų“). Pirmojo perskaičiavimo atveju laikotarpio pradžia (mėnuo) yra Sutarties įsigaliojimo dienos mėnuo. Antrojo ir vėlesnių perskaičiavimų atveju laikotarpio pradžia (mėnuo) yra paskutinio perskaičiavimo metu naudotos paskelbto atitinkamo indekso reikšmės mėnuo.

3.13. Skaičiavimams indeksų reikšmės imamos keturių skaitmenų po kablelio tikslumu. Apskaičiuotas pokytis (k) tolimesniems skaičiavimams naudojamas suapvalinus iki vieno skaitmens po kablelio, o apskaičiuotas įkainis „a_1“ suapvalinamas iki dviejų skaitmenų po kablelio.

3.14. Šalis, siekianti Sutarties kainos peržiūros, privalo raštu kreiptis į kitą Šalį ir prašyme pateikti visą reikalingą informaciją: Sutarties pavadinimą, numerį, datą, neperduotų ir neapmokėtų Prekių sąrašą su kiekiais, Indekso reikšmes su nuorodomis į viešus šaltinius Valstybės duomenų agentūros Oficialiosios statistikos portale arba kitus oficialius šaltinių duomenis, kita svarbi

informacija. Prašyme Šalis neturi teisės nurodyti kito Indekso ar prašyti perskaičiavimo pagal kitą Indeksą nei nurodytas šioje procedūroje.

3.15. Susitarimas turi būti sudarytas per 7 darbo dienas nuo Šalies pateikto tinkamo prašymo perskaičiuoti Sutarties kainą gavimo dienos.

3.16. Susitarimu Šalys neturi teisės keisti procedūroje nurodytos tvarkos ar kitų Sutarties nuostatų, išskyrus, jei keitimas atliekamas pagal Lietuvos Respublikos viešųjų pirkimų įstatymo nuostatas.

IV. ŠALIŲ ĮSIPAREIGOJIMAI

4.1. Pardavėjas įsipareigoja:

4.1.1. pateikti antivirusinės programinės įrangos licencijos raktą el. paštu its@palanga.lt ne vėliau nei per 5 darbo dienas po Sutarties pasirašymo;

4.1.2. užtikrinti, kad antivirusinės programinės įrangos licencija atitiktų Sutarties 2 priede keliamus reikalavimus;

4.1.3. už laiku neperduotas antivirusinės programinės įrangos licencijas sumokėti Pirkėjui netesybas, t. y. 0,02 proc. už kiekvieną uždelstą dieną nuo sutarties kainos.

4.2. Pirkėjas įsipareigoja:

4.2.1. už laiku pristatytas Prekes, sumokėti Pardavėjui per 30 dienų pagal gautus atsiskaitymo dokumentus (perdavimo–priėmimo aktą, PVM sąskaitą faktūrą) nuo jų gavimo dienos;

4.2.2. už ne laiku įvykdytą Sutarties 4.2.1 papunktį sumokėti Pirkėjui 0,02 proc. delspinigių nuo nesumokėtos sumos už kiekvieną uždelstą dieną.

V. SUTARTIES GALIOJIMO, PAKEITIMO IR NUTRAUKIMO SĄLYGOS

5.1. Sutartis įsigalioja Sutarties sudarymo dieną ir galioja iki prievolių pagal šią Sutartį įvykdymo.

5.2. Sutarties trukmė – 24 mėnesiai nuo Sutarties įsigaliojimo dienos arba iki visiško įsipareigojimų įvykdymo.

5.3. Sutarties sąlygos gali būti keičiamos tik vadovaujantis Viešųjų pirkimų įstatymo 89 straipsnio nuostatomis ir, kurias pakeitus, nebūtų pažeisti Viešųjų pirkimų įstatymo 17 straipsnyje nustatyti principai ir tikslai.

5.4. Sutartis gali būti nutraukiama Viešųjų pirkimų įstatymo 90 straipsnyje nustatytais atvejais.

VI. GINČŲ SPRENDIMAS, KITOS SĄLYGOS

6.1. Kilusius ginčus dėl Sutarties vykdymo Šalys sprendžia tarpusavio derybomis. Jeigu taip išspręsti ginčo nepavyksta, ginčas sprendžiamas Lietuvos Respublikos įstatymų nustatyta tvarka Lietuvos Respublikos teismuose.

6.2. Tuo atveju, jeigu kuri Sutarties nuostata yra ydinga, neatitinka teisės aktuose įtvirtintų nuostatų ar neturi teisinės galios, kitos Sutarties nuostatos teisinės galios nenustoja. Šalys turi pakeisti ydingąją, teisės aktų neatitinkančią ar teisės galios neturinčią nuostatą kita, artimiausia pagal prasmę negaliojančiai, teisiškai veiksminga nuostata.

6.3. Atsiradus nenumatytoms aplinkybėms (force majeure) Šalys neatsako už Sutartyje numatytų įsipareigojimų neįvykdymą arba netinkamą įvykdymą.

6.4. Pirkėjo paskirtas asmuo, atsakingas už Sutarties vykdymą – Arūnas Benetis, Komunikacijos ir e. paslaugų skyriaus vyresn. patarėjas, tel.: (0 460) 34 169, 0 620 50565, el. paštas arunas.benetis@palanga.lt.

6.5. Pardavėjo paskirtas asmuo, atsakingas už sutarties vykdymą – Andrius Gedminas, projektų vadovas, (0 46) 242 002, andrius.gedminas@csc.lt.

VII. ASMENS DUOMENŲ TVARKYMAS

7.1. Vykdydamos Sutartį Šalys įsipareigoja asmens duomenų tvarkymą vykdyti teisėtai – laikantis Bendrojo duomenų apsaugos reglamento 2016/679 (BDAR), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo ir kitų teisės aktų, reglamentuojančių asmens duomenų tvarkymą.

7.2. Šalių atstovų, darbuotojų ar kitų fizinių asmenų, pasitelktų Sutarčiai vykdyti duomenų tvarkymo teisėtumas grindžiamas būtinybe įvykdyti Sutartį arba būtinybe pasinaudoti iš Sutarties kylančiomis teisėmis.

7.3. Šalys asmens duomenis saugo ne ilgiau nei to reikalauja duomenų tvarkymo tikslai ar numato teisės aktai, jeigu juose yra nustatytas ilgesnis duomenų saugojimas. Asmens duomenys turi būti saugomi tol, kol iš sutartinių santykių gali kilti pagrįstų reikalavimų arba kiek tai reikalinga Šalių teisėtiems interesams įgyvendinti ir apsaugoti. Nebereikalingi asmens duomenys sunaikinami.

7.4. Gali būti tvarkomi šie Šalių vadovų, kitų darbuotojų, atsakingų asmenų ar atstovų, atstovaujančių Šalims, duomenys (I) vardas, pavardė; (II) kontaktiniai duomenys (darbo telefono numeris, darbo elektroninis paštas, darbovietės adresas; (III) užimamos pareigos; (IV) įgaliojimų (atstovavimo) duomenys, įskaitant atstovų asmens kodus, adresus; (V) Šalių vardu ir interesais vykdomas susirašinėjimas, ar kiti duomenys suformuojami Sutarties vykdymo metu.

7.5. Tvarkomus duomenis gali gauti: (I) Šalių darbuotojai, atsakingi už Šalių tarpusavio bendradarbiavimą ir ryšių palaikymą, taip pat vykdantys buhalterinės apskaitos, informacinių sistemų priežiūros, verslo rodiklių analitikos ir verslo planavimo funkcijas; (II) informacinių sistemų, kurias Šalys naudoja tarpusavio santykių valdymui, tiekėjai ir prižiūrėtojai; (III) mokesčių inspekcija; (IV) bankai; (V) Šalių pasitelkiami kiti asmenys, susiję su Sutarties vykdymu.

7.6. Jei Šalys ketina pasinaudoti kitų tolesnių duomenų tvarkytojų paslaugomis, Šalys perduos kitai Šaliai informaciją apie tolesnį duomenų tvarkytoją. Tokiu atveju, Šalys privalo užtikrinti, kad tolesnis duomenų tvarkytojas vykdys bent tuos pačius įsipareigojimus ir įgaliojimus, kuriuos ši Sutartis nustato. Taip pat Šalys supranta, kad jos pačios atsakys už tolesnių duomenų tvarkytojų veiksmus ir neveikimą.

7.7. Šalys įsipareigoja tinkamai informuoti visus fizinius asmenis (darbuotojus, įgaliotinius, valdymo organų narius, savo subtiekėju darbuotojus ir kitus atstovus), kurie bus pasitelkti Sutarčiai su Šalimis vykdyti, apie tai, kad jų asmens duomenys bus arba gali būti perduoti Šalims ir bus arba gali būti Šalių tvarkomi Sutarties vykdymo tikslais; kur ir kiek laiko asmens duomenys bus saugomi, ir kas turės galimybę su jais susipažinti. Šalys pažymi, kad fiziniai asmenys, kurie yra pasitelkti Sutarčiai su Šalimis vykdyti ir išvardinti Sutartyje, yra supažindinti su Sutartyje pateiktais jų asmeniniais duomenimis, ir Šalies nustatyta tvarka tam davė savo sutikimą.

7.8. Šalys šiuo susitaria, kad po Sutarties nutraukimo ar pasibaigimo, jos sunaikins arba grąžins visus joms patikėtus tvarkyti asmens duomenis pagal Sutartį ir jų kopijas, nebent Europos Sąjungos (ES) ar jų šalies įstatymai nustato reikalavimą saugoti asmens duomenis.

VIII. BAIGIAMOSIOS NUOSTATOS

8.1. Sutarties priedai yra neatskiriama Sutarties dalis.

8.2. Sutarčiai ir visoms iš šios Sutarties atsirandančioms teisėms ir pareigoms taikomi Lietuvos Respublikos įstatymai bei kiti norminiai teisės aktai, Sutartis turi būti aiškinama pagal Lietuvos Respublikos teisę.

8.3. Sutarties galiojimo laikotarpiu, Šalis inicijuojanti šios Sutarties sąlygų pakeitimą, pateikia kitai šaliai raštišką prašymą keisti Sutartį bei dokumentus, įrodančius aplinkybes, dėl kurių būtina keisti Sutarties sąlygas, argumentus, paaiškinimus, kopijas. Sutarties Šalims susitarus dėl sąlygų pakeitimo, šie keitimai įforminami rašytiniu susitarimu prie Sutarties, kuris yra neatsiejama Sutarties dalis.

8.4. Siekiant sunaudoti mažiau gamtos išteklių, pagal Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo, patvirtinto Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakymu Nr. D1-508 (Lietuvos Respublikos aplinkos ministro 2022 m. gruodžio 13 d. įsakymo Nr. D1-401 redakcija) (toliau – Tvarkos aprašas) 4.4.4.1 papunktį Šalys susitaria nerengti ir nenaudoti popierinių dokumentų, mažinti popieriaus sunaudojimą, atsisakyti nebūtino dokumentų kopijavimo ir spausdinimo. Su Sutarties vykdymu susiję dokumentai, t. y. pagal Sutartį teikiami užsakymai, susirašinėjimas, perdavimo ir priėmimo aktai, sąskaitos faktūros ir pan., pateikiami elektronine forma – tiesiogiai suformuoti elektroninėmis priemonėmis ar skaitmeninės originalo kopijos, Prekių perdavimo ir priėmimo aktai turi būti pasirašomi el. parašu. Išimtiniais atvejais su Sutarties vykdymu susiję dokumentai gali būti pateikiami popieriniu formatu, jeigu toks formatas privalomas pagal teisės aktus arba Pirkėjas nurodo tokį būtinumą – tokiu atveju turi būti naudojamas perdirbtas popierius, kuris atitinka minimaliuosius aplinkos apsaugos kriterijus, patvirtintus Tvarkos apraše.

8.5. Sutartis pasirašyta 2 (dviem) egzemplioriais lietuvių kalba, turinčiais vienodą juridinę galią.

8.6. Sutarties priedai:

8.6.1. Pardavėjo pasiūlymas (1 priedas);

8.6.2. techninė specifikacija (2 priedas).

IX. ŠALIŲ REKVIZITAI

PIRKĖJAS	PARDAVĖJAS
Palangos miesto savivaldybės administracija	UAB „CSC Telecom“
Vytauto g. 112, LT-00153 Palanga	Perkūnkiemio g. 7, LT-12131 Vilnius
Įmonės kodas 125196077	Įmonės kodas 111818067
Tel. (0 460) 48 705	Tel. (0 5) 210 1790
A. s. LT587180600002130301	A. s. LT237300010079267266
AB Šiaulių bankas	„Swedbank“, AB, banko kodas 73000
El. p. administracija@palanga.lt	El. p. info@csc.lt
Direktorė	Pardavimų vadovas
Ramunė Olšauskaitė Urbonienė	Tada Ivašauskas
_____ (parašas)	_____ (parašas)
A. V.	A. V.

UAB „CSC TELECOM“
Juridinio asmens kodas 111818067, Perkūnkiemio g. 7, Vilnius, tel. (8~5) 210 17 90, faks. (8~5) 213 17 95, duomenų tvarkytojas – valstybės įmonė Registrų centras

1 priedas

Palangos miesto savivaldybės administracija

PASIŪLYMAS
DĖL ANTIVIRUSINĖS PROGRAMOS LICENCIJOS ĮSIGIJIMO

Klaipėda
(vieta)
2025-03-14
(data)

Tiekėjo pavadinimas	UAB „CSC Telecom“
Tiekėjo adresas	Perkūnkiemio g. 7, Vilnius
Už pasiūlymą atsakingo asmens vardas, pavardė	Projektų vadovas Andrius Gedminas
Telefono numeris	+370 46 242002
El. pašto adresas	andrius.gedminas@csc.lt

Šiuo pasiūlymu pažymime, kad sutinkame su visomis pirkimo sąlygomis.

Mes siūlome:

1. Mes siūlome parduoti antivirusinės programos **ESET Protect Elite cloud** licencijas (150 vnt., toliau - Prekės), atitinkančias visas 2 priede nustatytas technines pirkimo sąlygas, už – 13200.00 Eur, PVM – 2772.00 Eur. Viso (į šią sumą įeina visos išlaidos ir visi mokesčiai) – 15972.00 Eur (penkiolika tūkstančių devyni šimtai septyniasdešimt du eurai ir 0 ct).

2. Prekes pristatyti per 5 darbo dienas nuo sutarties pasirašymo dienos, Vytauto g. 112, Palanga.

Pasiūlymas galioja iki 2025 m. birželio mėn. 30 d.

Projektų vadovas — parašas — Andrius Gedminas
Tiekėjo arba jo įgalioto asmens pareigos — vardas, pavardė

Dokumentą elektroniniu parašu
pasirašė ANDRIUS,GEDMINAS
Data: 2025-03-14 13:40:01

2 priedas

PATVIRTINTA
Palangos miesto savivaldybės administracijos
direktoriaus 2025 m. kovo 12 d. įsakymo
Nr. A1-307
2 punktu

ANTIVIRUSINĖS PROGRAMOS LICENCIJOS PIRKIMO TECHNINĖ SPECIFIKACIJA

I SKYRIUS
PIRKIMO OBJEKTAS

1. Antivirusinės programinės įrangos licencijų pirkimas. Kadangi perkamos nematerialaus pobūdžio intelektinės prekės, todėl, vadovaujantis Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakymo „Dėl aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo patvirtinimo“ Nr. D1-508 4.4.3 papunkčiu, pirkimas laikomas žaliu. Pirkimas vykdomas bendra tvarka, kadangi centrinė perkančioji organizacija Viešoji įstaiga CPO LT tokių paslaugų neteikia.

II SKYRIUS
PIRKIMO OBJEKTO APIBŪDINIMAS

2. Palangos miesto savivaldybės administracija norėdama užtikrinti informacinių sistemų ir skaitmeninio turto apsaugą nuo kibernetinių atakų planuoja įsigyti antivirusinę programinę įrangą.

III SKYRIUS
TECHNINIAI REIKALAVIMAI

3. Minimalūs techniniai reikalavimai antivirusinei programinei įrangai:

Eil. nr.	Parametras	Minimali reikšmė
1	*2*	*3*
1.	Licencijų skaičius	150 vnt.
2.	Programinės įrangos tipas	• Kompiuterinių darbo vietų, serverių, mobiliųjų ir planšetinių įrenginių apsauga nuo virusų ir šnipinėjimo programų, su ugniasiene ir pašto apsauga; • centralizuotai valdomas darbo vietų kietųjų diskų šifravimas; • papildoma apsauga nuo išpirkos reikalaujančių kenkėjų ir nulinės dienos atakų su debesyje valdoma „smėliadėžės“ technologija. Kompiuterinių darbo vietų ir serverių ankstyvojo kibernetinių grėsmių aptikimo ir užkardymo programinė įranga su centralizuotu valdymu (angl. *Extended Detection and Response, XDR*); • centralizuotai valdoma apsauga Microsoft 365 (Exchange Online, OneDrive, Teams ir Sharepoint Online) debesijos aplikacijoms;

1	*2*	*3*
		• centralizuotai valdomas dviejų veiksnių (angl. *Two Factor Authentication, 2FA*) autentifikavimas; • centralizuotai valdomas pažeidžiamumų ir programų pataisų valdymo modulis; • visi programinės įrangos sprendimai privalo būti valdomi iš vieno gamintojo administravimo konsolės(-ių) debesijoje arba organizacijos tinkle.
3.	Programinės įrangos gamintojas	• Turi būti nurodytas. • siekiant visapusiško suderinamumo vykdant centralizuotą stebėseną ir valdant visas išplėstines antivirusinės infrastruktūros apsaugos sistemas, visa programinė įranga turi būti pagaminta to paties gamintojo.
4.	Programinės įrangos paketo pavadinimas	• Turi būti nurodytas.
5.	Palaikomos operacinės sistemos	• Kompiuterinės darbo vietos: - Microsoft Windows 11 64-bitų; - Microsoft Windows 10 32-bitų ir 64-bitų; - Ubuntu Desktop 20.04 LTS 64-bitų ir naujesnės versijos. • Mobilieji įrenginiai: - Android 10 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). • Linux serveriai: - RedHat Enterprise Linux (RHEL) 7, 8 ir 9 versijos; - Ubuntu Server 18.04 LTS, 20.04 LTS, 22.04 LTS ir 24.04 LTS versijos; - Debian 10 ir 11 versijos; - SUSE Linux Enterprise Server (SLES) 12 ir 15 versijos; - Oracle Linux 8 ir 9 versijos; - Amazon Linux 2 versija. • 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 2019 64-bitų; - Microsoft Windows Server 2022 64-bitų; - Ubuntu Server 20.04 LTS; - Debian 10.

1	*2*	*3*
		• Turi palaikyti 2FA įgalinimą šioms Microsoft operacinėms sistemoms: - Windows 10 (įskaitant 22H2 atnaujinimą); - Windows 11 (įskaitant 22H2 atnaujinimą); - Windows Server 2012; - Windows Server 2012 R2; - Windows Server 2012 Essentials; - Windows Server 2012 R2 Essentials; - Windows Server 2016; - Windows Server 2016 Essentials; - Windows Server 2019; - Windows Server 2019 Essentials; - Windows Server 2022. • Linux: RHEL, Debian, Ubuntu, SLED, SLES, OpenSUSE, Fedora ir bei dauguma kitų RPM ir DEB paketų valdymu pagrįstų platinamų programų. • Nuotolinė saugumo sprendimų administravimo konsolė(-ės) turi būti suderinama su naršyklėmis: - Mozilla Firefox; - Microsoft Edge; - Google Chrome; - Opera.
6.	Palaikomos operacinės sistemos ir duomenų bazės ankstyvojo kibernetinių grėsmių aptikimo ir užkardymo programinei įrangai	• Kompiuterinės darbo vietos: - Microsoft Windows 10 32-bitų ir 64-bitų; - Microsoft Windows 11 32-bitų ir 64-bitų; - RedHat Enterprise Linux (RHEL) 8 ir 9 versijos; - Ubuntu 18.04 LTS ir naujesnės versijos; - SUSE Linux Enterprise Desktop 15 versija. • Serveriai: - Microsoft Windows Server 2012 64-bitų; - Microsoft Windows Server 2012 R2 64-bitų; - Microsoft Windows Server 2016 64-bitų; - Microsoft Windows Server 2019 64-bitų; - Microsoft Windows Server 2022 64-bitų; - RedHat Enterprise Linux (RHEL) 8 ir 9 versijos; - Ubuntu Server 18.04 LTS ir naujesnės versijos; - Debian 10 ir 11 versijos; - SUSE Linux Enterprise Server (SLES) 15 versija; - Oracle Linux 8 ir 9 versijos; - Amazon Linux 2 versija. • Nuotolinio administravimo konsolė (diegiant organizacijos viduje) turi palaikyti diegimą į: - Microsoft Windows Server 2019 64-bitų; - Microsoft Windows Server 2022 64-bitų; - Ubuntu Server 20.04 LTS; - Debian 10. • Nuotolinio administravimo konsolė turi būti suderinama su duomenų bazėmis: - MySQL 8.0.31 ir naujesnėmis; - Microsoft SQL Server 2017 ir naujesnėmis.

1	*2*	*3*
7.	Veikimo kokybės reikalavimai	• Programinės įrangos gamintojas turi turėti bent ISO 9001:2015 ir ISO 27001:2013 standartus atitinkančias sertifikacijas; • gamintojas turi būti įvertintas AV comparatives „Anti-Phishing Certification Test 2024" rinkos tyrime; • kibernetinių grėsmių aptikimo analizė turi būti pagrįsta pagal MITRE ATT&CK® metodologiją; • gamintojas turi būti įvertintas/sertifikuotas „Endpoint Prevention & Response (EPR) Test 2024 – AV Comparatives" tyrime; • gamintojas turi būti įvertintas/sertifikuotas „Advanced Threat Protection Test 2024 – Enterprise – AV comparatives" tyrime.
8.	Administravimo konsolės(-ių) aktyvavimas ir diegimas	• Turi būti galimybė administravimo konsolę(-es) debesyje aktyvuoti 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.
9.	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 apsaugos aktyvacijai reikia: - palaikomo Microsoft 365 prenumeratos plano; - administratoriaus prieiga prie Azure Active Directory; - prieiga prie Azure Cloud Services – Exchange (mail) | OneDrive paskyros; - prieiga prie gamintojo teikiamo paslaugų valdymo puslapio debesijos sprendimuose.
10.	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.

1	*2*	*3*
11.	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.
12.	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;

1	*2*	*3*
		• turi būti apsauga nuo brute-force atakų; • darbo vietų ugniasienės valdymas turi būti atliekamas centralizuotai administravimo konsolės pagalba.
13.	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.
14.	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 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“.
15.	Funkciniai reikalavimai dviejų veiksnių autentifikacijos (2FA) sprendimui	• 2FA turi būti valdomas naudojant valdymo konsolę; • 2FA autentifikacijos modulis turi leisti naudoti jau sukurtas arba sukurti naujas saugumo politikas; • 2FA autentifikacijos modulis turi leisti apsaugoti: - prieigą prie įmonės virtualiojo privataus tinklo (VPN); - nuotolinio darbalaukio protokolą (nuotolinį RDP prisijungimą); - papildomą autentifikaciją kompiuterio prisijungimui (prisijungimą prie operacinės sistemos); - saityno/debesijos kompiuterija paremtas paslaugas, kurioms naudojama Microsoft ADFS 3.0, tokios kaip Office 365: ▪ Microsoft Web Apps, tokias kaip OWA; ▪ Exchange Control Panel ir Exchange Administrator Center; ▪ VMware Horizon View; ▪ RADIUS paremtas paslaugas; ▪ Exchange valdymą ir Exchange administratorių

1	*2*	*3*
		centrą. • Programinė įranga turi suteikti kelias vartotojų autentifikavimo galimybes prisijungti prie kompiuterių ar paslaugų, apsaugotų dviejų veiksnių autentifikacija, tokias kaip: - vienkartinis slaptažodis, gaunamas SMS žinutėmis; - vienkartinis slaptažodis, sugeneruotas dedikuotoje mobiliojoje aplikacijoje; - vienkartinis slaptažodis, kuris pasikeičia po jo panaudojimo (HOTP); - vienkartinis slaptažodis, kuris pasikeičia periodiškai po tam tikro laiko intervalo (TOTP); - vienkartinis slaptažodis, perduodamas el. paštu; - autentifikavimas vienu paspaudimu mobiliojoje aplikacijoje; - aparatinės įrangos autentifikatorius (Hard Tokens); - FIDO protokolo autentifikacija. • Saugumo nustatymai turi leisti: - įjungti/išjungti 2FA autentifikaciją; - suteikti galimybę vartotojui pasirinkti autentifikacijos būdą (-us) savarankiškos registracijos metu; - nustatyti maksimalų leistinų bandymų prisijungti prie darbo vietos skaičių. • Sistemos administratoriui naudojant valdymo konsolę turi būti galimybė: - inicijuoti vartotojo atkūrimo rakto sukūrimą (master recovery key); - įjungti/išjungti vartotojo autentifikacijos metodus, pvz.: vienkartinis slaptažodis, gaunamas SMS žinutėmis, autentifikaciją per mobiliąją aplikaciją, Hard Tokens, FIDO; - laikinai užblokuoti arba visai panaikinti prieigą prie 2FA autentifikacijos; - importuoti vartotojus iš failo: CSV arba LDF; - turi palaikyti centralizuotą administravimą nuotoliniu būdu per interneto naršyklę. • Jeigu programa yra įdiegta Active Directory aplinkoje, ji turi saugoti duomenis Active Directory duomenų saugykloje kaip atsargines kopijas; • valdymo konsolė turi leisti pridėti vartotojus ir įrenginius prie valdymo konsolės naudojant šiuos metodus: - sinchronizavimą su Active Directory/LDAP; - rankiniu būdu įvedus vartotojo telefono numerį, el. pašto adresą ir kt. • serveris turi leisti įdiegti saugumo sprendimus nuotoliniu būdu ir be vartotojo įsikišimo; • valdymo konsolė turi leisti sinchronizuoti Active Directory vartotojų medį arba sukurti atskirą grupę; • turi palaikyti savarankiškos registracijos (Self-enrollment) funkciją; • valdymo konsolė turi leisti nuotoliniu būdu vizualizuoti šią

1	*2*	*3*
		vartotojų informaciją: - pagrindinė vartotojo informacija; - vartotojo statusas; - autentifikavimo istorija; - autentifikavimo konfigūracija; - perspėjimai. • turi turėti galimybę įtraukti IP adresus į baltąjį sąrašą (IP address whitelisting); • turi turėti centralizuotą bendrosios politikos(-ų) nustatymą visiems programinės įrangos vartotojams; • turi turėti antrinio autentifikavimo serverio nustatymo galimybę – nustojus veikti vienam autentifikavimo serveriui, veikimas automatiškai turi pereiti kitam nuotolinio autentifikavimo serveriui; • pagal numatytuosius nustatymus serveris turi pateikti keletą standartinių ataskaitų bei leisti kurti naujus ataskaitų šablonus; • valdymo konsolės sąsaja turi dirbti su informacijos skydais. Jie turi būti visiškai interaktyvūs ir leisti atlikti reikiamas užduotis iš kelių sekcijų.
16.	Funkciniai reikalavimai pažeidžiamumų ir programų pataisų valdymo moduliui	• Pažeidžiamumų ir programų pataisų valdymo modulis turi turėti: - automatinį saugumo spragų nuskaitymą; - prioritetų nustatymą pagal pavojingumą; - filtravimo parinktis; - pažeidžiamumų išimtis; - paveiktų įrenginių sąrašą; - automatinį ir rankinį saugumo spragų užkardymą/pataisymą; - pritaikomas taisymo/pataisų valdymo politikas; - galimų pataisymų sąrašą.
17.	Funkciniai reikalavimai Microsoft 365 aplinkos apsaugai	• Antiviruso modulis (Anti-Malware) – programinė įranga, sauganti nuo virusų, šnipinėjimo programų ir kitų kenkėjiškų failų, grėsmių; • turi būti apsauga nuo šlamšto (Antispam) – draudžianti pasiekti šlamšto ir sukčiavimo el. laiškus; • turi būti apsauga nuo sukčiavimo (Anti-Phishing) – draudžianti vartotojams pasiekti tinklalapių, žinomų dėl sukčiavimo; • turi skenuoti POP3, IMAP, MAPI ir HTTP protokolus nuo kenkėjiško turinio; • turi turėti galimybę siųsti šifruotus „Syslog“ pranešimus į naudotojo nustatytus tinklo įrenginius CEF, LEEF ir json formatais; • automatinis homoglifų aptikimas ir blokavimas (angl. *Homoglyph Detection*) el. laiškuose.
18.	Funkciniai reikalavimai mobiliųjų įrenginių valdymo moduliui	• Turi palaikyti centralizuotą administravimą nuotoliniu būdu; • valdymas turi būti įgyvendintas saugumo sprendimų administravimo konsolėje kuriant politikas, kurias galima

1	*2*	*3*
		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.
19.	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.
20.	Funkciniai reikalavimai saugumo sprendimų 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;

1	2	3
		- patentuota 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 (angl. *trigger*), 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 ne daugiau kaip 10 nesėkmingų bandymų prisijungti iš to paties IP adreso, serveris turi laikinai blokuoti tolesnius bandymus prisijungti iš šio IP adreso; • po ne daugiau kaip 15 nesėkmingų bandymų vedant

1	*2*	*3*
		netinkamą seanso ID iš to paties IP adreso, serveris turi laikinai blokuoti tolesnius bandymus prisijungti iš šio IP adreso; • turi būti galimybė nustatyti automatinę agento atnaujinimo funkciją.
21.	Funkciniai reikalavimai ankstyvojo kibernetinių grėsmių aptikimo ir užkardymo valdymo konsolei	• Turi palaikyti centralizuotą administravimą nuotoliniu būdu. Serveris turi komunikuoti su galiniais įrenginiais per agentą, kuris gali saugoti politiką ir kaupti žurnalinius įrašus, kol įrenginys yra neprisijungęs; • interneto konsolės sąsaja turi dirbti su informacijos skydais; • turi būti stebėsenos skydelis, kuriame galima stebėti naujausią informaciją apie įmonės tinkle įvykusius įtartinus įvykius; • turi būti interaktyviai atvaizduojami įspėjimai, teikiami pagal taisykles apie įtartinus įvykius, kurie įvyko veikiant programinei įrangai; • turi būti numatytųjų taisyklių sąrašas ir galimybė parengti savo taisykles, kuriomis būtų apibūdinamas įtartinas programinės įrangos veikimas; • turi būti automatiškai vykdomas įspėjimų paskirstymas pagal kritiškumo lygį, leidžiant greitai nustatyti ir reaguoti į kritinius įvykius; • turi būti galimybė nustatyti prioritetinius įspėjimus, kad būtų lanksčiau rūšiuojami ir filtruojami įvykiai; • turi būti galimybė grupuoti įspėjimus pagal skirtingus kriterijus, pvz., tipą, kompiuterį, taisyklę, procesą, rinkmeną; • turi būti galimybė užfiksuoti su informacijos saugumu susijusius incidentus sudarant įtartinus aptikimus, kuriuose būtų pateikta informacijos apie įvykį santrauka (data, laikas ir kur įvykis įvyko (kompiuteris), kuris vartotojas paleido vykdomąjį failą ir koks konkretus procesas sukėlė paleidimą) ir išsami informacija apie kiekvieną iš išvardytų parametrų; • kiekviename įtartiname aptikime turi būti numatytas specialus informacijos skyrius, kuriame pateiktas išsamus taisyklę suaktyvinusio įvykio aprašymas, galimų priežasčių, pavojų ir pasekmių sąrašas bei rekomendacijos dėl būtinų veiksmų tolesnei įvykio analizei vykdyti; • aptikus kritinius incidentus, turi būti galimybė gauti informaciją apie žinomų būdų ir priemonių, kurias anksčiau naudojo įsilaužėliai panašiose situacijose, sąrašą su nuorodomis į atitinkamas MITRE ATT&CK® šaltinio nuorodas, kur galima rasti išsamesnės informacijos apie įsilaužimų taktikas; • turi būti įtartinų aptikimų interaktyvioji sąsaja, leidžianti išsamiau išnagrinėti su informacijos saugumu susijusį incidentą naudojant pagrindinius parametrus, kurie yra prieinami bendrajame įtartiname aptikime; • turi būti pateikiama išsami informacija apie taisyklę

1	2	3
		suaktyvinusį procesą, pvz., procesų medis, failų sistemos ir operacinės sistemos registro pakeitimai, tinklo veikla, ryšiai su URL adresais, papildomai atsisiųsti vykdomieji failai ir išsamus operacinės sistemos įvykių žurnalas; • turi būti galimybė sukurti išsamias atskirų įvykių išimtis, kurios turėtų apimti informaciją apie vykdomųjų failų kontrolines sumas (angl. *hash checksum*), jų buvimo vietą, skaitmeninį parašą (angl. *signature*) ir kt.; • turi būti galimybė įtraukti pasirinktus EXE/DLL failus į užblokuotųjų sąrašą remiantis kontroline suma, tokiu būdu inicijuojant blokavimą darbo vietose ir serveriuose; • turi būti galimybė nuotoliniu būdu ištrinti visus įtartinus EXE/DLL failus ir perkelti juos į karantiną; • turi būti galimybė atsisiųsti įtartinus failus iš darbo vietų ir serverių tolesnės analizės vykdymui; • turi būti galimybė parengti visų EXE/DLL failų, esančių darbo vietose ir serveriuose, sąrašą tolesnės analizės vykdymui; • turi būti galimybė parengti baltuosius (angl. *whitelist*)/ juoduosius (angl. *blacklist*) EXE/DLL failų sąrašus; • turi būti galimybė peržiūrėti išsamią informaciją apie EXE/ DLL failus, su jais susijusius įspėjimus, naudojimo statistiką, failų pakeitimus, registrą, sukurtus tinklo ryšius; • turi būti galimybė esant poreikiui atkurti, ištrinti ir atsisiųsti užblokuotų EXE/DLL failų sąrašą išsamesnės analizės vykdymui; • turi būti automatiškai vykdomas EXE/DLL failų paskirstymas pagal kritiškumo lygį, leidžiant greitai nustatyti ir reaguoti į įtartiną failų elgesį; • turi būti galimybė žymėti EXE/DLL failus kaip patikimus ar saugius ir kaip patikrintus bei išanalizuotus; • turi būti galimybė tiesiogiai iš konsolės vykdyti papildomos informacijos apie failus sparčiąją paiešką trečiųjų šalių ištekliuose, tokiuose kaip „Virus Total“ arba lygiaverčiuose; • turi būti galimybė parengti visų skriptų, kurie buvo vykdomi darbo vietose ir serveriuose, sąrašą; • turi būti galimybė grupuoti skriptus pagal skirtingus kriterijus, tokius kaip pirminis procesas, pirmasis antrinis procesas, komandinė eilutė; • turi būti galimybė žymėti patikrintus skriptus kaip patikimus ar saugius; • turi būti galimybė gauti su skripto turiniu susijusią informaciją apie pasitelktus EXE/DLL failus, procesus, sugeneruotus antrinių procesų sąrašus, failų pakeitimus, registrus, užmegztus tinklo ryšius; • turi būti automatiškai vykdomas skriptų paskirstymas pagal kritiškumo lygį, leidžiant greitai nustatyti ir reaguoti į įtartiną elgesį; • turi būti galimybė atvaizduoti kompiuterių sąrašą ir išsamią informaciją apie veiksmus, EXE/DLL failus ir skriptus;

1	*2*	*3*
		• turi būti galimybė nuotoliniu būdu atlikti darbo vietos perkrovimą arba visiškai ją išjungti; • turi būti galimybė iš nuotolinės valdymo konsolės darbo vietai paleisti antivirusinės programos greitąjį skenavimą; • turi būti galimybė iš nuotolinės valdymo konsolės atlikti darbo vietos operacinės sistemos būsenos momentinę nuotrauką, kurioje būtų užfiksuota informacija apie visus tuo metu vykstančius procesus ir tinklo ryšius, bei pateikiama informacija apie kritinį operacinės sistemos registro turinį, operacinės sistemos planavimo priemonės užduotis, operacinės sistemos vartotojus ir jų privilegijas, operacinės sistemos kritinių failų, pvz., „hosts“, „win.ini“ ir kt., turinį, bei visa išsami informacija apie operacinę sistemą ir įdiegtą programinę įrangą; • turi būti galimybė kurti ir išsaugoti paieškos užduotis visoje duomenų bazėje, kurioje renkami duomenys iš visų valdomų kompiuterių, įskaitant bet kokius parametrus (net kelis simbolius iš vykdomosios komandinės eilutės) ir naudojant įvairius filtrus.
22.	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 saugumo sprendimų centralizuotą administravimo konsolę.
23.	Atnaujinimai	• Klientinės dalies programinė įranga privalo turėti funkcionalumą parsisiųsti atnaujinimus tiesiai iš: - gamintojo atnaujinimų serverio; - centralizuoto valdymo serverio; - kitų klientų. • klientinės dalies programinė įranga privalo turėti funkcionalumą veikti kaip atnaujinimų serveris kitiems klientams tam, kad būtų galima taupyti tinklo pralaidumo resursus; • turi būti galimybė nustatyti automatinę saugumo produkto atnaujinimo funkciją.
24.	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.
25.	Versija	• Turi būti siūloma naujausia stabili programinės įrangos versija, oficialiai gamintojo paskelbta internete.
26.	Dokumentacija	• Turi būti pateikta aktuali dokumentacija, apimanti programinės įrangos įdiegimo, bendro naudojimo, administravimo, sistemos atstatymo procedūras.
27.	Gamintojo aptarnavimo	• Gamintojo atstovas turi teikti nemokamą pagalbą, konsultacijas telefonu, kreipiantis į pagalbos centrą darbo

1	*2*	*3*
	(angl. support) sąlygos	dienomis darbo valandomis lietuvių kalba; • gamintojo atstovas turi suteikti 2 valandas konsultacijų produkto diegimo ir atnaujinimo klausimais, kurios turi būti įvykdytos ne vėliau kaip 30 dienų nuo licencijų aktyvavimo dienos; • gamintojo atstovas turi teikti nemokamą pagalbą, konsultacijas telefonu, kreipiantis į pagalbos centrą darbo dienomis darbo valandomis lietuvių kalba.
28.	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.

4. Minimalūs reikalavimai antivirusinės programinės įrangos veikimo techninio palaikymo ir kibernetinės saugos paslaugoms:

Eil. nr.	Parametras	Techniniai reikalavimai
1	*2*	*3*
1.	Paslaugų teikimo trukmė	• 6 mėn. nuo sutarties pasirašymo.
2.	Kibernetinės saugos paslaugų apimtis darbo vietų ir serverių saugumo produktams	• Saugumo produktui neaptikus galimai kenksmingos programinės įrangos (angl. *malware*) faile, URL, domene ar pagal IP adresą, turi būti teikiama pagalba analizuojant incidentą ir, jei aptinkamas kenkėjas, pateikiama informacija apie kenkėjiškų programų šeimą, pridedamas aptikimas; • įvykus išpirkos reikalaujančios programinės įrangos (angl. *ransomware*) incidentui, turi būti teikiama pagalba identifikuojant išpirkos reikalaujančios programinės įrangos tipą, įvertinant jos išplitimo mastą, pateikiant incidento suvaldymo ir prevencijos rekomendacijas ir, jei įmanoma, dešifratorių; • saugumo produktui aptikus, tačiau nepavykus pašalinti kenkėjiškų failų, turi būti teikiama pagalba jų pašalinimui arba alternatyvi valymo programa tokių failų panaikinimui; • saugumo produktui galimai klaidingai blokuojant (angl. *false positive*) failą, URL, domeną arba IP adresą, turi būti teikiama pagalba analizuojant pateiktus duomenis ir nustačius, kad aptikta klaidingai, pašalinti aptikimą arba sukurti išimtį; • perkančiajai organizacijai kilus įtarimams dėl trečiųjų šalių programinės įrangos veikimo ir siekiant įvertinimo iš saugumo pusės, turi būti teikiama pagalba analizuojant programos elgesį ir siūlant galimą sprendimą, remiantis įtartino elgesio apibūdinimu ir kitais duomenimis.

1	*2*	*3*
3.	Kibernetinės saugos paslaugų apimtis XDR saugumo produktui	• Paslaugos teikimo metu turi būti teikiama pagalba konfigūruojant, atnaujinant ir optimizuojant XDR saugumo produktą; • paslaugos teikimo metu turi būti teikiama pagalba kuriant reagavimo taisykles ir išimtis; • paslaugos teikimo metu turi būti teikiama pagalba identifikuojant be failų vykdomas atakas (angl. *fileless attacks*) į darbo vietas bei serverius; • paslaugos teikimo metu turi būti teikiama pagalba atliekant incidento pirminę failų analizę išanalizavus paveiktos aplinkos duomenis pateikiant rekomendacijas dėl tolimesnių veiksmų; • perkančiajai organizacijai turi būti teikiamos konsultacijos atliekant grėsmių tyrimą ar pagrindinių priežasčių analizę, bei patarimai, kaip ištaisyti trūkumus, nenaudojant papildomų vidinių išteklių.
4.	Reagavimo laikai techninio palaikymo ir kibernetinės saugos paslaugų teikimui	• Įprasto, aukšto, kritinio prioriteto klaidos ar užklausos reagavimo laikas pagal galimybes. Perkančiajai organizacijai pateikiant atsakymą turi sudaryti problemos sprendimas, papildomų duomenų prašymas arba tolesnių veiksmų nustatymas.
5.	Prieigos prie gamintojo žinių bazės reikalavimai	• Turi būti teikiama 24/7 (visą parą) internetinė prieiga prie ESET gamintojo žinių bazės; • žinių bazės turinys turi būti prieinamas lietuvių arba anglų kalbomis.
6.	Prieigos prie gamintojo sistemų būsenos portalo reikalavimai	• Turi būti teikiama 24/7 (visą parą) internetinė prieiga prie ESET gamintojo sistemų būsenos portalo.
7.	Kreipimosi į Klientų aptarnavimo centrą būdai	• Turi būti el. paštu ir telefonu.
8.	Paslaugų teikimo kalba	• Turi būti lietuvių arba anglų kalbomis.
9.	Reikalavimai darbo vietų ir serverių klaidų ar užklausų teikimui	• Turi būti suteikta galimybė teikti įprasto (pagalba sprendžiant nekritines problemas, netrikdančias įprasto tinklo veikimo, teikiant atsakymus į bendruosius konfigūracinius klausimus), aukšto ir kritinio prioriteto (pagalba sprendžiant kritines problemas, trikdančias perkančiosios organizacijos veiklą, konsultuojant dėl kompleksinio problemos sprendimo, produktų atnaujinimo) klaidas ar užklausas; • problemos išsprendimo laikas kiekvienu konkrečiu atveju turi būti suderinamas su Perkančiąja organizacija;
10.	Reikalavimai XDR klaidų ar užklausų teikimui	• Turi būti suteikta galimybė teikti žemo (pagalba kuriant taisykles ir išimtis, sprendžiant bendruosius konfigūracinius, optimizavimo klausimus) ir aukšto bei kritinio prioriteto (pagalba tiriant skaitmeninį incidentą, atnaujinant produktus) klaidas ar užklausas; • problemos išsprendimo laikas kiekvienu konkrečiu atveju

1	*2*	*3*
		turi būti suderinamas su perkančiąja organizacija.
11.	Reikalavimai nuotolinėms sesijoms ir konsultacijoms	• Turi būti numatyta galimybė sutarties galiojimo laikotarpiu perkančiosios organizacijos IT administratoriams per 1 mėn. turėti iki 1 sesijos dedikuoto laiko aptikimų aptarimui su Klientų aptarnavimo centro inžinieriais; • turi būti suteikta galimybė sutarties galiojimo laikotarpiu perkančiosios organizacijos IT administratoriams turėti diegimo ir atnaujinimo veiklą iki 1 vnt. per metus su Klientų aptarnavimo centro inžinieriais; • turi būti suteikta galimybė sutarties galiojimo laikotarpiu perkančiosios organizacijos IT administratoriams turėti esamos situacijos įvertinimo veiklą iki 1 vnt. per metus su Klientų aptarnavimo centro inžinieriais.
12.	Reikalavimai Klientų aptarnavimo centrui	• Klientų aptarnavimo centro paslaugos turi būti teikiamos darbo dienomis nuo 8.00 iki 17.00 val.; • siekiant užtikrinti sklandų paslaugų teikimą, Klientų aptarnavimo centro ne mažiau kaip du inžinieriai yra sertifikuoti teikti šias paslaugas (pagal perkančiosios organizacijos pareikalavimą pateikti kvalifikaciją pagrindžiančius sertifikatus).
13.	Prieigos prie gamintojo el. mokymų platformos reikalavimai	• Turi būti teikiama 24/7 (visą parą) internetinė prieiga prie siūlomo produkto (antivirusinės programinės įrangos) gamintojo mokymų platformos; • mokymų turinys ir egzaminas prieinamas lietuvių arba anglų kalba; • turi būti perkančiosios organizacijos IT administratoriams (iki 2 asmenų) suteikta prieiga prie siūlomo produkto (antivirusinės programinės įrangos) pradedančiųjų mokymų kurso ir išlaikius egzaminą turi būti suteiktas gamintojo sertifikatas; • turi būti perkančiosios organizacijos IT administratoriams (iki 2 asmenų) suteikta prieiga prie siūlomo produkto (antivirusinės programinės įrangos) pažengusiųjų mokymų kurso ir išlaikius egzaminą turi būti suteiktas gamintojo sertifikatas; • turi būti perkančiosios organizacijos IT administratoriams (iki 2 asmenų) suteikta prieiga prie eksperto mokymų kurso ir išlaikius egzaminą turi būti suteiktas gamintojo sertifikatas; • turi būti numatyta galimybė gamintojo išduotus sertifikatus parsisiųsti PDF formatu tiesiai iš el. mokymų platformos.

IV SKYRIUS
PREKIŲ PATEIKIMO IR ATSISKAITYMO UŽ JAS TERMINAI

5. Antivirusinės programinės įrangos licencijų raktas pateikiamas ne vėliau nei per 5 darbo dienas po sutarties pasirašymo ir galioja 24 mėn. nuo perdavimo–priėmimo akto pasirašymo ir PVM sąskaitos faktūros gavimo dienos.

6. Už antivirusinės programinės įrangos licencijas pirkėjas sumoka iš Palangos miesto savivaldybės 2025–2027 metų strateginio veiklos plano, patvirtinto Palangos miesto savivaldybės tarybos 2025 m. sausio 30 d. sprendimu Nr. T2-9 „Dėl Palangos miesto savivaldybės 2025–2027 metų strateginio veiklos plano patvirtinimo“, Bendrosios programos 1.1.2.1 priemonės „Kompiuterizuotų darbo vietų atnaujinimas ir plėtojimas“ per 30 kalendorinių dienų nuo PVM sąskaitos faktūros gavimo dienos.

7. Vykdant pirkimo sutartį, PVM sąskaitos faktūros, sąskaitos faktūros, išankstinės sąskaitos, kreditiniai ir debetiniai dokumentai turi būti teikiami naudojantis informacinės sistemos SABIS priemonėmis. Kiti išlaidas pagrindžiantys dokumentai gali būti teikiami naudojantis informacinės sistemos SABIS priemonėmis. Prisijungti prie elektroninės paslaugos SABIS galima interneto adresu https://sabis.nbfc.lt/. Paslauga yra apmokama Lietuvos Respublikos finansų ministro nustatyta tvarka. Vykdytojas įsipareigoja išankstinėse sąskaitose, PVM sąskaitose faktūrose nurodyti sutarties, kurios pagrindu išrašomos sąskaitos, numerį.

V SKYRIUS
INFORMACIJA, KAIP TURI BŪTI APSKAIČIUOTA IR PATEIKTA PASIŪLYME NURODOMA PIRKIMO KAINA

8. Bendra kaina nurodoma eurais (be PVM, PVM ir kaina su PVM). Į šią sumą turi įeiti visos išlaidos ir mokesčiai.

9. Pagrindinis paslaugos pirkimo vertinimo kriterijus – mažiausia pasiūlyta kaina.

VI SKYRIUS
PREKĖS PATEIKIMO VIETA

10. Palangos miesto savivaldybės administracija, Vytauto g. 112, Palanga.

_____

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Palangos miesto savivaldybės administracija
Dokumento sudarytojas (-ai)	UAB "CSC Telecom"
Dokumento pavadinimas (antraštė)	Antivirusinės programinės įrangos įsigijimas
Dokumento registracijos data ir numeris	2025-03-21 Nr. (2.13 E) S6-K-94
Dokumento gavimo data ir dokumento gavimo registracijos numeris	-
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Ramunė Olšauskaitė Urbonienė Direktorė
Parašo sukūrimo data ir laikas	2025-03-20 15:51
Parašo formatas	Einamojo galiojimo (XAdES-EPES)
Laiko žymoje nurodytas laikas	
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016
Sertifikato galiojimo laikas	2020-05-25 15:37 - 2025-05-24 23:59
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	IVAŠAUSKAS,TADAS -
Parašo sukūrimo data ir laikas	2025-03-20 18:21
Parašo formatas	Einamojo galiojimo (XAdES-EPES)
Laiko žymoje nurodytas laikas	
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016
Sertifikato galiojimo laikas	2023-10-08 08:50 - 2026-10-08 08:50
Parašo paskirtis	Registravimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Beata Liutikienė Vedėjas
Parašo sukūrimo data ir laikas	2025-03-21 13:48
Parašo formatas	Trumpalaikio galiojimo (XAdES-T)
Laiko žymoje nurodytas laikas	2025-03-21 13:48
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016
Sertifikato galiojimo laikas	2021-11-10 13:38 - 2026-11-09 23:59
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	-
Pagrindinio dokumento priedų skaičius	2
Pagrindinio dokumento pridedamų dokumentų skaičius	0
Pridedamo dokumento sudarytojas (-ai)	-
Pridedamo dokumento pavadinimas (antraštė)	1 priedas CSC Pasiulymas 20250314-s0314.pdf
Pridedamo dokumento registracijos data ir numeris	-
Pridedamo dokumento sudarytojas (-ai)	-
Pridedamo dokumento pavadinimas (antraštė)	2 priedas Tech spec.docx
Pridedamo dokumento registracijos data ir numeris	-
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Elpako v.20250312.1
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Tikrinant dokumentą nenustatyta jokių klaidų (2025-03-27)
Elektroninio dokumento nuorašo atspausdinimo data ir ją atspausdinęs darbuotojas	2025-03-27 nuorašą suformavo Rasa Morkūnienė
Paieškos nuoroda	-
Papildomi metaduomenys	-