PREKIŲ VIEŠOJO PIRKIMO–PARDAVIMO SUTARTIS NR. Reg. Nr.

Reg. data
Vilnius

Lietuvos Respublikos Vyriausybės kanceliarija (toliau – Užsakovas), atstovaujama Vyriausybės kanclerio pavaduotojo Almino Mačiulio, veikiančio pagal Vyriausybės kanclerio 2021 m. vasario 23 d. įsakymą Nr. V-27 „Dėl apskaitos ir kitų dokumentų pasirašymo ir apskaitos organizavimo“ (Vyriausybės kanclerio 2022 m. gegužės 23 d. įsakymo Nr. V-99 redakcija), ir **Blue Bridge MSP, UAB** (toliau – Tiekėjas), atstovaujama pardavimų direktoriaus Gintauto Bazio, veikiančio pagal įgaliojimą, kartu vadinamos šalimis, o atskirai Šalimi, atsižvelgdamos į tai, kad Tiekėjas laimėjo Užsakovo skelbtą viešąjį pirkimą (pirkimo Nr. 626915) (Tinko ugniasienės įrangos viešojo pirkimo komisijos 2022-10-26 posėdžio protokolas Nr. 67-152, pagrindinis kodas pagal Bendrąjį viešųjų pirkimų žodyną – 32420000-3, papildomas kodas – 72260000-5), sudarė šią prekių viešojo pirkimo–pardavimo sutartį (toliau – Sutartis):

1. Sutarties objektas

1.1. Sutarties objektas – Tinklo ugniasienės įranga, jos diegimo ir 36 mėn. palaikymo paslaugos, pagal techninėje specifikacijoje (Sutarties 2 priedas) nustatytus reikalavimus (toliau – prekės ir paslaugos).

2. Sutarties kaina ir atsiskaitymo tvarka

2.1. Bendra Sutarties kaina be PVM 80 350,00 Eur (aštuoniasdešimt tūkstančių trys šimtai penkiasdešimt eurų), PVM – 16 873,50 Eur (šešiolika tūkstančių aštuoni šimtai septyniasdešimt trys eurai ir 50 centų), bendra Sutarties kaina su PVM – 97 223,50 Eur (devyniasdešimt septyni tūkstančiai du šimtai dvidešimt trys eurai ir 50 centų). Į bendrą Sutarties kainą įskaičiuoti visi mokesčiai ir visos Tiekėjo išlaidos, susijusios su šios Sutarties vykdymu, įskaitant sąskaitų teikimo per „E-sąskaita“ sistemą mokestį.

2.2. Prekių ir paslaugų pirkimui taikomas fiksuotos kainos apskaičiavimo būdas. Sutarties kaina Sutarties galiojimo metu nebus keičiama.

2.3. Atsiskaitoma su Tiekėju už tinkamas ir laiku pristatytas prekes ir suteiktas paslaugas į Tiekėjo rekvizituose nurodytą sąskaitą ne vėliau kaip per 10 darbo dienų nuo PVM sąskaitos faktūros informacinės sistemos „E. sąskaita“ priemonėmis gavimo dienos. PVM sąskaitos faktūros išrašymo pagrindas yra Sutarties šalių pasirašytas prekių ir paslaugų perdavimo-priėmimo aktas. Prekių ir paslaugų perdavimo-priėmimo aktas pasirašomas, jeigu prekės ir paslaugos atitinka Sutarties reikalavimus, pristatytos ir įdiegtos laiku, suteikta 36 mėn. palaikymo paslaugų garantija, yra tinkamos ir kokybiškos, taip pat yra įvykdyti kiti Sutartiniai įsipareigojimai. Išrašydamas PVM sąskaitą faktūrą Tiekėjas turi nurodyti Sutarties datą ir numerį.

3. Šalių teisės ir pareigos

3.1. **Tiekėjas įsipareigoja:**

3.1.1. ne vėliau kaip per 3 mėnesius nuo Sutarties įsigaliojimo dienos pristatyti tinkamas ir kokybiškas prekes ir jas įdiegti, po įdiegimo suteikti 36 mėn. prekių palaikymo garantiją;

3.1.2. užtikrinti, kad prekės ir paslaugos atitiktų visus techninėje specifikacijoje nurodytus reikalavimus: prekės būtų pilnai sukomplektuotos, atitiktų techninius reikalavimus ir pan., o paslaugos būtų teikiamos kokybiškai ir laiku;

3.1.3. atlyginti tiesioginius nuostolius Užsakovui jei būtų pristatytos netinkamos ir (ar) nekokybiškos prekės ar netinkamai ar ne laiku teikiamos paslaugos, o Užsakovas dėl to patirtų žalą;

3.1.4. vykdyti Užsakovo teisėtus nurodymus, susijusius su Sutarties vykdymu;

3.1.5. visiškai atlyginti Užsakovui nuostolius, jeigu Tiekėjas, jo darbuotojai ir kiti su Tiekėju susiję asmenys nesilaikytų Lietuvos Respublikos įstatymų ir kitų teisės aktų ir dėl to Užsakovui būtų pateikti kokie nors reikalavimai ar pradėti procesiniai veiksmai ar Užsakovas patirtų žalą;

3.1.6. išsaugoti visą Sutarties ir gautą iš Užsakovo informaciją, be Užsakovo sutikimo nenaudoti tokios informacijos ir jos neatskleisti jokiam kitam asmeniui, išskyrus asmenis, paskirtus vykdyti Sutartį. Sutarties turinys tokiems asmenims atskleidžiamas tik tiek, kiek to reikia Sutarties vykdymo tikslams. Šis įsipareigojimas yra netaikomas, kai Lietuvos Respublikoje galiojančiuose teisės aktuose nustatyta tvarka informacijos apie pirkimą (taip pat ir Sutartį) pareikalauja teisėsaugos, kontrolės ir kitos institucijos, turinčios tokią teisę;

3.1.7. tinkamai, kokybiškai ir laiku vykdyti įsipareigojimus, numatytus Sutartyje ir kituose Lietuvos Respublikoje galiojančiuose teisės aktuose;

3.1.8. ištaisyti savo sąskaita bet kokius trūkumus, susijusius prekių tiekimu ir paslaugų teikimu pagal Sutartį;

3.1.9. užtikrinti, kad sutartį vykdys tik tokią teisę turintys asmenys;

3.1.10. užtikrinti, kad tiekiamos prekės ir teikiamos paslaugos, Tiekėjo ir jo pasitelkiamų subtiekėjų interesai nekels grėsmės nacionaliniam saugumui;

3.1.11. laikytis techninėje specifikacijoje (Sutarties 2 priedas) nustatytų aplinkosauginių reikalavimų ir Asmens duomenų tvarkymo minimalių techninių ir organizacinių priemonių (Sutarties 1 priedas);

3.1.12. Tiekėjas turi ir kitų Sutartyje ir Lietuvos Respublikoje galiojančiuose teisės aktuose numatytų pareigų.

3.2. **Tiekėjas turi teisę:**

3.2.1. prašyti, kad Užsakovas pateiktų dokumentus ar kitą informaciją, būtinus Sutarčiai tinkamai įvykdyti;

3.2.2. reikalauti, kad Užsakovas priimtų kokybiškai ir laiku pristatytas prekes ir suteiktas paslaugas, atitinkančias Sutarties ir teisės aktų reikalavimus, ir sumokėtų už jas Sutartyje nustatyta tvarka;

3.2.3. gauti apmokėjimą Sutartyje nustatyta tvarka, jeigu jis tinkamai, kokybiškai ir laiku vykdo Sutartį;

3.2.4. Tiekėjas turi ir kitų Sutartyje ir Lietuvos Respublikoje galiojančiuose teisės aktuose numatytų teisių.

3.3. **Užsakovas įsipareigoja:**

3.3.1. Sutarties vykdymo metu bendradarbiauti su Tiekėju ir suteikti Tiekėjui Sutarčiai vykdyti pagrįstai reikalingą informaciją;

3.3.2. paskirti asmenis, atsakingus už Sutarties vykdymą;

3.3.3. priimti tinkamas ir laiku pristatytas prekes ir suteiktas paslaugas bei apmokėti Tiekėjui Sutartyje nustatyta tvarka;

3.3.4. Užsakovas turi ir kitų Sutartyje ir Lietuvos Respublikoje galiojančiuose teisės aktuose numatytų pareigų.

3.4. **Užsakovas turi teisę:**

3.4.1. kontroliuoti Sutarties vykdymą ir duoti Tiekėjui nurodymus, kad būtų tinkamai, kokybiškai ir laiku įvykdyta Sutartis;

3.4.2. atsisakyti priimti prekes ir paslaugas, kurios neatitinka Sutartyje nustatytų reikalavimų;

3.4.3. nemokėti Tiekėjui už netinkamai, nekokybiškai ir (ar) ne laiku pristatytas prekes ir suteiktas paslaugas;

3.4.4. Užsakovas turi ir kitų Sutartyje ir Lietuvos Respublikoje galiojančiuose teisės aktuose numatytų teisių.

4. Sutarties galiojimas, vykdymas, keitimas

4.1. Sutartis įsigalioja Sutarties šalims ją pasirašius ir galioja iki visiško šalių įsipareigojimų įvykdymo arba jos nutraukimo Lietuvos Respublikos teisės aktuose ar Sutartyje nustatytais atvejais ir tvarka.

4.2. Sutartis jos galiojimo laikotarpiu gali būti keičiama vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymo 89 straipsniu. Sutarties sąlygų pakeitimai įforminami šalių rašytiniais susitarimais, kurie yra neatsiejama Sutarties dalis.

4.3. Tiekėjas, norėdamas pakeisti pasiūlyme nurodytus Sutartį vykdančius specialistus, privalo ne vėliau kaip prieš 3 darbo dienas iki šių asmenų pakeitimo raštu (el. paštu) pateikti naujų specialistų sąrašą. Naujai siūlomi specialistai privalo turėti ne žemesnę nei pirkimo sąlygose nurodytą kvalifikaciją. Užsakovas privalo per 2 darbo dienas el. paštu pritarti dėl Sutartį vykdančių specialistų pakeitimo arba pateikti pastabas Tiekėjui.

4.4. Jei bet kuri šios Sutarties nuostata tampa ar pripažįstama visiškai ar iš dalies negaliojanti, tai neturi įtakos kitų Sutarties nuostatų galiojimui.

4.5. Sutarties galiojimo termino pabaiga neatleidžia Sutarties šalių nuo civilinės atsakomybės už Sutarties pažeidimą.

5. Šalių atsakomybė ir sutarties nutraukimas

5.1. Šalis, prieš 10 darbo dienų įspėjusi raštu kitą Šalį, gali nutraukti Sutartį, jei ji nevykdo ar netinkamai įvykdo sutartinius įsipareigojimus ir tai yra esminis Sutarties pažeidimas. Nustatydamos esminį Sutarties pažeidimą šalys privalo vadovautis Lietuvos Respublikos civilinio kodekso 6.217 straipsnio nuostatomis.

5.2. Sutartis gali būti nutraukta abipusiu raštišku šalių susitarimu.

5.3. Užsakovas turi teisę vienašališkai nutraukti Sutartį, nesant Tiekėjo kaltės, raštu įspėjęs Tiekėją prieš 15 kalendorinių dienų. Tokiu atveju Užsakovas įsipareigoja atsiskaityti su Tiekėju už iki Sutarties nutraukimo pristatytas prekes ir suteiktas paslaugas bei atlyginti Tiekėjo patirtus tiesioginius nuostolius.

5.4. Kai nutraukiama Sutartis, Užsakovas, dalyvaujant Tiekėjui ar jo atstovams, inventorizuoja pristatytas prekes ir suteiktas paslaugas. Taip pat parengiama ataskaita apie Sutarties nutraukimo dieną esančius šalių įsiskolinimus.

5.5. Sutarties nutraukimas nepanaikina teisės reikalauti atlyginti nuostolius, atsiradusius dėl Sutarties neįvykdymo bei netesybas.

5.6. Jeigu Sutartis nutraukiama dėl Tiekėjo kaltės, Užsakovo patirti nuostoliai ar išlaidos gali būti išieškomi išskaičiuojant juos iš Tiekėjui mokėtinos sumos.

5.7. Jei Tiekėjas vėluoja vykdyti sutartinius įsipareigojimus per Sutartyje ar Užsakovo nurodytą terminą, Užsakovas turi teisę be oficialaus įspėjimo ir nesumažindamas kitų savo teisių gynimo būdų pradėti skaičiuoti 0,03 % dydžio delspinigius nuo nepristatytų prekių ir nesuteiktų paslaugų kainos už kiekvieną Sutartyje numatytų įsipareigojimų nevykdymo dieną. Užsakovas turi teisę išskaičiuoti delspinigius iš Tiekėjui mokėtinos sumos. Delspinigių sumokėjimas neatleidžia Tiekėjo nuo Sutarties įsipareigojimų vykdymo.

5.8. Jei Užsakovas dėl savo kaltės neatlieka apmokėjimo per Sutartyje nurodytą terminą, Tiekėjui raštu pareikalavus, Užsakovas moka Tiekėjui 0,03 % dydžio delspinigius nuo neapmokėtos sumos už faktiškai pristatytas, tinkamas, kokybiškas ir pagal prekių perdavimo aktą priimtas prekes ir suteiktas paslaugas už kiekvieną uždelstą dieną. Delspinigiai skaičiuojami iki apmokėjimo dienos.

6. Subtiekėjai ir jų keitimo tvarka

6.1. Tiekėjas turi teisę Sutarčiai vykdyti pasitelkti subtiekėjus. Sudarius Sutartį, tačiau ne vėliau negu Sutartis pradedama vykdyti, Tiekėjas įsipareigoja Užsakovui pranešti tuo metu žinomų subtiekėjų pavadinimus, kontaktinius duomenis ir jų atstovus. Tiekėjas bet kokiu atveju atsako už visus pagal Sutartį prisiimtus įsipareigojimus, nepaisant to, kad jiems vykdyti bus pasitelkiami tretieji asmenys.

6.2. Sutarties vykdymo metu Tiekėjas gali pakeisti subtiekėjus arba pasitelkti naujus. Apie tai Tiekėjas turi informuoti Užsakovą, nurodydamas subtiekėjo pakeitimo ar pasitelkimo priežastis. Pakeisti arba pasitelkti nauji subtiekėjai privalo pateikti subtiekėjo pašalinimo pagrindų nebuvimą patvirtinančius dokumentus. Gavęs tokį pranešimą, Užsakovas, jei nėra subtiekėjo pašalinimo pagrindų, kartu su Tiekėju sudaro susitarimą dėl subtiekėjų pakeitimo. Jį pasirašo abi Sutarties šalys. Šis susitarimas yra laikomas neatskiriama Sutarties dalimi. Tiekėjas negali vienašališkai keisti ar pasitelkti naujų subtiekėjų, apie tai neinformavęs Užsakovo ir tokio pakeitimo neįforminęs susitarimu dėl Sutarties pakeitimo. Jei pakeisto subtiekėjo padėtis atitinka bent vieną pagal Lietuvos Respublikos viešųjų pirkimų įstatymo 46 straipsnį nustatytą pašalinimo pagrindą, Užsakovas reikalauja, kad Tiekėjas per Užsakovo nustatytą terminą pakeistų minėtą subtiekėją reikalavimus atitinkančiu subtiekėju.

6.3. Užsakovas gali tiesiogiai atsiskaityti su subtiekėjais. Apie šią galimybę Užsakovas subtiekėją informuoja atskiru pranešimu per 3 darbo dienas nuo informacijos iš Tiekėjo apie pasitelkiamą subtiekėją gavimo dienos. Norėdamas pasinaudoti tiesioginio atsiskaitymo galimybe, subtiekėjas turi ne vėliau kaip per 2 darbo dienas raštu pateikti prašymą Užsakovui. Tokiu atveju Užsakovas, Tiekėjas ir subtiekėjas sudaro trišalę sutartį, kurioje pateikiama tiesioginio atsiskaitymo su subtiekėju tvarka, atsižvelgiant į Sutartyje ir subtiekimo sutartyje nustatytus reikalavimus, įskaitant teisę Tiekėjui prieštarauti nepagrįstiems mokėjimams. Trišalės sutarties dėl tiesioginio atsiskaitymo su subtiekėju pasirašymas nekeičia Tiekėjo atsakomybės dėl Sutarties vykdymo.

7. Ginčų sprendimas

7.1. Visi ginčai dėl šios Sutarties vykdymo bus sprendžiami derybų būdu. Nepavykus išspręsti ginčo derybomis, ginčas sprendžiamas Lietuvos Respublikos teisme pagal Užsakovo buveinės vietą.

8. Nenugalimos jėgos aplinkybės

8.1. Šalis gali būti visiškai ar iš dalies atleidžiama nuo atsakomybės dėl aplinkybių, kurių ji negalėjo kontroliuoti bei protingai numatyti sutarties sudarymo metu ir negalėjo užkirsti kelio šių aplinkybių ar jų pasekmių atsiradimui – nenugalimos jėgos (force majeure), Šalies įrodytos pagal Lietuvos Respublikos Civilinį kodeksą, Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimą Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių patvirtinimo“ ir Lietuvos Respublikos Vyriausybės 1997 m. kovo 13 d. nutarimą Nr. 222 „Dėl Nenugalimos jėgos (force majeure) aplinkybes liudijančių pažymų išdavimo tvarkos patvirtinimo“. Šalis, negalinti laiku įvykdyti savo sutartinių įsipareigojimų dėl nenugalimos jėgos aplinkybių, turi kuo greičiau, bet ne vėliau kaip per vieną dieną nuo aplinkybių paaiškėjimo dienos raštu informuoti apie tai kitą Šalį. Šalis, pažeidusi nurodytą terminą, atleidžiama nuo atsakomybės tik nuo to momento, kada kita Šalis gavo jos pranešimą apie nenugalimos jėgos aplinkybes.

9. Asmens duomenų tvarkymas

9.1. Kiekviena Šalis kitos Šalies pateiktus jos darbuotojų, įgaliotų asmenų, subrangovų darbuotojų ar kitų atstovų, taip pat kitų asmenų duomenis tvarkys tik šios Sutarties vykdymo, teisėto intereso siekiant pareikšti ar apsiginti nuo ieškinių ar kitų reikalavimų, kylančių dėl Sutarties vykdymo, o taip pat siekiant įvykdyti Šaliai taikomuose teisės aktuose numatytas pareigas, tikslais bei juos atitinkančiais teisiniais pagrindais, įskaitant Bendrojo duomenų apsaugos reglamento (ES) 2016/679 5 straipsnyje įtvirtintus su asmens duomenų tvarkymu susijusius principus.

9.2. Kiekviena Šalis kitos Šalies pateiktus 9.1 papunktyje nurodytus asmens duomenis saugos visą Sutarties galiojimo laikotarpį, o taip pat po jos pasibaigimo – tiek, kiek būtina pareikšti ar apsiginti nuo ieškinių ar kitų reikalavimų, įvykdyti Šaliai taikomuose teisės aktuose numatytas pareigas. Pasibaigus asmens duomenų saugojimo terminui, jie bus sunaikinami, jeigu galiojantys teisės aktai nenustatys kitaip.

9.3. Kiekviena Šalis kitos Šalies pateiktus 9.1 papunktyje nurodytus asmens duomenis gali teikti šiems duomenų gavėjams: techninės ir programinės įrangos, naudojamos asmens duomenų tvarkymui, ir su tuo susijusių paslaugų teikėjams, Šalies naudojamų informacinių ir ryšių technologijų priežiūrą ir aptarnavimą vykdantiems paslaugų teikėjams, buhalterinės apskaitos ir kitiems paslaugų teikėjams, kitiems duomenų gavėjams, kuriems asmens duomenys turi būti teikiami siekiant tinkamai vykdyti Sutartį arba vadovaujantis Šaliai taikomais teisės aktų reikalavimais. Tiekėjas šios Sutarties 9.1 papunktyje nurodytus Užsakovo pateiktus asmens duomenis gali teikti asmenims, kuriuos jis turi teisę pasitelkti šios Sutarties vykdymui. Užsakovas viešųjų pirkimų metu pateikto pasiūlymo, preliminarios sutarties (jei ji buvo sudaryta) ir šios Sutarties bei minėtų sutarčių pakeitimų skaitmenines kopijas skelbs viešai (išskyrus viešai neskelbtinus asmens duomenis) Centrinėje viešųjų pirkimų informacinėje sistemoje, kurios duomenų valdytoja yra Viešųjų pirkimų tarnyba.

9.4. Kiekviena Šalis įsipareigoja visus fizinius asmenis, kurių asmens duomenis tvarko, laikydamasi Bendrojo duomenų apsaugos reglamento (ES) 2016/679 13 ir 15 straipsnių nuostatų, tinkamai informuoti apie jų asmens duomenų tvarkymą (įskaitant jų asmens duomenų perdavimą kitai Šaliai) ir šių asmenų pagal Bendrąjį duomenų apsaugos reglamentą (ES) 2016/679 turimas teises. Informacija apie Užsakovo atliekamą asmens duomenų tvarkymą ir duomenų subjektų teisių įgyvendinimą skelbiama Užsakovo interneto svetainėje www.lrvk.lrv.lt.

10. Kitos sąlygos

10.1. Nė viena iš Sutarties šalių neturi teisės perduoti trečiajam asmeniui teisių ir įsipareigojimų pagal šią Sutartį be raštiško kitos Šalies sutikimo.

10.2. Visi Sutartyje neaptarti klausimai sprendžiami vadovaujantis Lietuvos Respublikos teisės aktais.

10.3. Už Sutarties vykdymą bei prekių perdavimo-priėmimo akto pasirašymą atsakingi asmenys:

Užsakovo atsakingas asmuo	Tiekėjo atsakingas asmuo

10.4. Už Sutarties ir jos pakeitimų paskelbimą Centrinėje viešųjų pirkimų informacinėje sistemoje atsakingas asmuo – Lietuvos Respublikos Vyriausybės kanceliarijos Administravimo departamento Viešųjų pirkimų skyriaus patarėjas Jonas Šniaukšta.

10.5. Sutartis sudaryta lietuvių kalba dviem vienodą teisinę galią turinčiais egzemplioriais – po vieną kiekvienai Šaliai.

10.6. Sutarties šalys patvirtina, kad Sutartį perskaitė, suprato jos turinį ir pasekmes, priėmė ją kaip atitinkančią jų tikslus ir pasirašė.

10.7. Visi Sutarties priedai pasirašius Sutartį tampa neatskiriama Sutarties dalimi. Sutarties pakeitimai ir papildymai galioja tik tuomet, jeigu yra patvirtinti Sutarties šalių parašais.

10.8. Sutarties priedai:

10.8.1. Sutarties 1 priedas – Asmens duomenų tvarkymo minimalios techninės ir organizacinės priemonės;

10.8.2. Sutarties 2 priedas – techninė specifikacija;

10.8.3. Sutarties 3 priedas – Tiekėjo pasiūlymas.

11. Šalių rekvizitai

Tiekėjas:
Blue Bridge MSP, UAB
Įmonės kodas: 301489547
Adresas: J. Jasinskio g. 16A, 03163 Vilnius
Tel. 8 5 252 6060
El. p.: info@bluebridge.lt
Ats. sąsk. Nr. LT89 2140 0300 0280 5128
Bankas: Luminor Bank AS
Banko kodas: 40100
PVM mokėtojo kodas: LT100003708514

Pardavimų direktorius
Gintautas Bazys

Užsakovas:
Lietuvos Respublikos Vyriausybės kanceliarija
Įstaigos kodas: 188604574
Adresas: Gedimino pr. 11, 01103 Vilnius
Tel. +370 5 2663711
El. p. lrvkanceliarija@lrv.lt
Ats. sąsk. Nr. LT33 7300 0100 8338 8034
Bankas: Swedbank, AB
Banko kodas: 73000
Įstaiga nėra PVM mokėtoja

Vyriausybės kanclerio pavaduotojas
Alminas Mačiulis

2022 m. lapkričio d. sutarties
Nr. LRVK- 1 priedas

ASMENS DUOMENŲ TVARKYMO MINIMALIOS TECHNINĖS IR ORGANIZACINĖS PRIEMONĖS

1. Minimalios organizacinės saugumo priemonės, kurias Tiekėjas privalo įdiegti ir užtikrinti, kad jų būtų laikomasi yra šios:

1.1. Saugumo valdymas:

1.1.1. Saugumo politika. Tiekėjas turi nustatyti dokumentuotą asmens duomenų saugumo politiką ir kasmet ją peržiūrėti, kiek reikalinga.

1.1.2. Vaidmenys ir atsakomybė. Vaidmenys ir atsakomybės, susijusios su asmens duomenų tvarkymu, turi būti aiškiai apibrėžtos ir paskirstytos vadovaujantis saugumo politika. Keičiantis darbuotojams, teisių ir atsakomybės atšaukimo tvarka turi būti aiškiai apibrėžta, numatant ir aiškias jų perdavimo procedūras.

1.1.3. Prieigos valdymo politika. Specialios prieigos kontrolės teisės turi būti priskirtos kiekvienam vaidmeniui, susijusiam su asmens duomenų tvarkymu, pagal būtinumo žinoti principą.

1.1.4. Pakeitimų valdymas. Tiekėjas turi užtikrinti, kad visi informacinių sistemų pakeitimai būtų registruojami ir stebimi konkretaus asmens (pvz., IT skyriaus ar saugumo darbuotojo). Šis procesas turi būti reguliariai prižiūrimas. Programinės įrangos tobulinimas turi būti atliekamas specialioje aplinkoje, kuri nebūtų sujungta su sistema, kurioje tvarkomi asmens duomenys. Kai reikalingas testavimas, turi būti naudojami išgalvoti (ne tikrieji) duomenys, o kai tai neįmanoma, galima testavimui naudoti tikruosius subjektų duomenis suderinus su Užsakovu, užtikrinant asmens duomenų apsaugą.

1.1.5. Duomenų tvarkytojai. Kai Tiekėjas pasitelkia kitus duomenų tvarkytojus, jis privalo turėti nustatytas ir dokumentuotas gaires ir procedūras, reguliuojančias kitų duomenų tvarkytojų atliekamą duomenų tvarkymą, kurios būtų taikomos kitiems duomenų tvarkytojams. Šios procedūros turi privalomai nustatyti tokį patį duomenų apsaugos lygį kaip ir Tiekėjo saugumo politikoje. Tiekėjas turi įpareigoti kitus duomenų tvarkytojus nedelsiant pranešti Tiekėjui apie asmens duomenų saugumo pažeidimus, taip pat pateikti įrodymus dėl tinkamų saugumo priemonių įgyvendinimo.

1.2. Incidentų valdymas:

1.2.1. Asmens duomenų saugumo pažeidimai ir incidentai. Tiekėjas privalo turėti reagavimo į saugumo incidentus planą su detaliomis procedūromis. Apie duomenų saugumo pažeidimus nedelsiant turi būti informuojama vadovybė.

1.3. Žmogiškieji ištekliai:

1.3.1 Konfidencialumo įsipareigojimai. Tiekėjas privalo užtikrinti, kad visi darbuotojai suprastų savo pareigas ir atsakomybę, susijusią su duomenų tvarkymu. Vaidmenys ir pareigos turi būti aiškiai išdėstyti darbuotojams prieš pradedant vykdyti jiems priskirtas funkcijas ir darbus.

1.3.2. Mokymai. Tiekėjas privalo užtikrinti, kad visi darbuotojai būtų tinkamai informuoti apie informacinės sistemos saugumo kontrolę, kuri susijusi su jų kasdieniu darbu. Darbuotojai, kurių darbas susijęs su asmens duomenų tvarkymu, turi būti informuojami apie atitinkamus asmens duomenų apsaugos reikalavimus ir teisinius įpareigojimus rengiant reguliarius mokymus, informavimo renginius ar instruktažus.

2. Minimalios techninės saugumo priemonės Tiekėjo vidinėms sistemoms, kurias privalo įdiegti ir užtikrinti, kad jų būtų laikomasi yra šios:

2.1. Prieigų kontrolė ir autentifikavimas. Tiekėjas turi įdiegti prieigų kontrolės sistemą, taikomą visiems vartotojams, prieinantiems prie informacinių technologijų sistemų, kuri leistų kurti, patvirtinti, peržiūrėti ir pašalinti naudotojų paskyras. Turi būti vengiama naudoti bendras naudotojų paskyras. Vietose, kur bendra naudotojų paskyra yra būtina, turi būti užtikrinta, kad visi bendros paskyros naudotojai turi tokias pat teises ir pareigas. Turi būti įdiegtas autentifikavimo mechanizmas, suteikiantis prieigą prie informacinės sistemos pagal prieigų kontrolės politiką. Autentifikavimui turi būti naudojamas bent jau naudotojo prisijungimo vardas ir slaptažodis, kuris atitiktų nustatytą sudėtingumo lygį. Prieigų kontrolės sistema turi gebėti nustatyti slaptažodžius, kurie neatitinka sudėtingumo lygio ir neleisti jų naudoti. Vartotojo slaptažodžiai turi būti saugomi naudojant kodavimo formą (*angl. hash form*).

2.2. Techninių žurnalų įrašai ir stebėsena. Techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai, taikomajai programai, naudojamai asmens duomenų tvarkymui, ir turi fiksuoti visus prieigos prie asmens duomenų veiksmus. Rekomenduojamas saugojimo terminas – ne mažiau kaip 6 mėnesiai. Techninių žurnalų įrašai turi turėti laiko žymas ir būti apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos. IT sistemose naudojami laiko apskaitos mechanizmai turi būti sinchronizuoti pagal bendrą laiko atskaitos šaltinį. Visi sistemų administratorių ir operatorių veiksmai (taip pat ir jų atliekamas vartotojo teisių papildymas, panaikinimas, keitimas) turi būti registruojami. Turi būti neįmanoma ištrinti ar pakeisti techninių įrašų turinio. Prieiga prie įrašų taip pat turi būti registruojama, siekiant atlikti neįprastų veiksmų susekimo stebėseną.

2.3. Tarnybinių stočių, duomenų bazių apsauga. Duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų korektiškai ir naudotų atskirą paskyrą su priskirtomis žemiausiomis operacinės sistemos privilegijomis. Duomenų bazės ir taikomųjų programų tarnybinės stotys turi apdoroti tik tuos asmens duomenis, kurie yra reikalingi darbui, atitinkančiam duomenų apdorojimo tikslus.

2.4. Darbo stočių apsauga. Kompiuterinėse darbo vietose naudotojams turi būti apribota galimybė išjungti ar apeiti, išvengti saugumo nustatymų. Antivirusinės taikomosios programos ir aptikimo žymenys turi būti atnaujinami ne rečiau kaip kas savaitę. Naudotojams negalima turėti privilegijų diegti, šalinti, administruoti neautorizuotos programinės įrangos. IT sistemos turi turėti nustatytą sesijos laiką, t. y. naudotojui esant neaktyviam sistemoje nustatytą laiką, sesija privalo būti nutraukta. Rekomenduojamas neaktyvios sesijos laikas – ne daugiau kaip 15 min. Kritiniai operacinės sistemos saugos atnaujinimai, išleidžiami operacinės sistemos gamintojo, turi būti įdiegiami reguliariai ir nedelsiant.

2.5. Tinklų ir komunikacijos sauga. Visais atvejais, kai prieiga prie naudojamų IT sistemų yra vykdoma internetu, ryšys turi būti šifruojamas kriptografiniais protokolais (pvz., TLS). Belaidis ryšys prie IT sistemų turi būti leidžiamas tik tam tikriems vartotojams ir procesams. Belaidžio ryšio potinklis turi būti atskirtas nuo kitų potinklių. Belaidė prieiga turi būti apsaugota patikimais šifravimo mechanizmais. Nuotolinė prieiga prie IT sistemų galima organizacijos paskirtam darbuotojui kontroliuojant ir stebint jos veikimą per iš anksto nustatytus įrenginius. Bet koks judėjimas iš, į IT sistemą turi būti stebimas ir kontroliuojamas naudojant ugniasienes ir įsibrovimo (įsilaužimo) aptikimo sistemas.

2.6. Programinės įrangos sauga. Informacinės sistemose naudojama programinė įranga, skirta asmens duomenims tvarkyti, turi atitikti programinės įrangos saugos gerąją praktiką, programinės įrangos kūrime taikomą saugos gerąją praktiką, programinės įrangos kūrimo struktūras, standartus. Specifiniai saugos reikalavimai turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose. Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos. Programinės įrangos kūrimo, testavimo ir verifikacijos etapai turi vykti atsižvelgiant į pagrindinius

saugos reikalavimus. Prieš paleidžiant programinę įrangą, turi būti atliktas šios įrangos pažeidžiamumo, pritaikomumo ir infrastruktūros atsparumo skverbimuisi įvertinimas. Programinė įranga negali būti patvirtinta, kol nėra pasiektas reikiamas saugumo lygis. Turi būti atliekami periodiški infrastruktūros atsparumo skverbimuisi testavimai. Programinės įrangos atnaujinimai turi būti ištestuoti ir įvertinti prieš juos diegiant į darbo aplinką atitinkamomis veiklos sąlygomis.

2.7. Fizinė sauga. Informacinės sistemos infrastruktūros perimetras turi būti neprieinamas neautorizuotam personalui. Įsilaužimo (įsibrovimo) aptikimo sistemos turi būti įdiegtos visose saugumo zonose. Laisvos saugios zonos turi būti fiziškai rakinamos ir periodiškai patikrinamos. Tarnybinių stočių patalpoje turi būti įdiegta automatinė gaisro gesinimo sistema, uždara valdoma oro kondicionavimo sistema ir nepertraukiamo maitinimo šaltinis. Išorės subjektų personalui, įgyvendinančiam teikiamas palaikymo ar garantines paslaugas, turi būti suteikta ribota prieiga prie saugių zonų.

3. Atsižvelgiant į pavojaus duomenų saugumui lygį, Tiekėjas turi pasirinkti griežtesnes saugumo priemones, kad būtų užtikrinta tinkama duomenų apsauga.

2022 m. lapkričio d. sutarties
Nr. LRVK- 2 priedas

TECHNINĖ SPECIFIKACIJA

1. Bendrieji reikalavimai

1.1. ***Pirkimo objektas – tinklo ugniasienės įranga, jos diegimo ir 36 mėn. palaikymo paslaugos.***

1.2. Įrangos pristatymo ir įdiegimo terminas – 3 mėnesiai nuo Sutarties įsigaliojimo dienos.

1.3. Perkama Įranga privalo būti nauja ir nenaudota, pateikiama originalioje gamintojo pakuotėje, gamykliškai atnaujinti komponentai („Refurbished“) neleistini.

1.4. Pardavėjas turi užtikrinti, kad Įrangos gamintojas nėra paskelbęs apie siūlomos Įrangos gamybos arba tobulinimo nutraukimą (pvz. „End of life time“ ar „Discontinued“).

1.5. Tiekėjas turi būti oficialus siūlomų prekių gamintojo atstovas (jeigu tiekėjas pats nėra siūlomų prekių gamintojas) ir turi turėti teisę parduoti siūlomą įrangą. Kartu su pasiūlymu tiekėjas privalo pateikti patvirtinančius dokumentus: siūlomų prekių gamintojo sertifikatą arba kitus lygiaverčius įrodymus, patvirtinančius, kad Tiekėjas yra gamintojo oficialus ir sertifikuotas atstovas, įgaliotas parduoti Užsakovui reikalingas prekes.

1.6. Tiekėjo siūlomos prekės ir paslaugos turi nekelti grėsmės nacionaliniam saugumui.

1.7. Užsakovas laikys, kad prekės ir paslaugos kelia grėsmę nacionaliniam saugumui, kai:

1.7.1. įrangos gamintojas ar jį kontroliuojantis asmuo yra registruoti (jeigu gamintojas ar jį kontroliuojantis asmuo yra fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) Lietuvos Respublikos viešųjų pirkimų įstatymo (toliau – VPĮ) 92 straipsnio 14 dalyje numatytame sąraše nurodytose valstybėse ar teritorijose (sąrašas patvirtintas Lietuvos Respublikos Vyriausybės 2022 m. kovo 30 d. nutarimu Nr. 280 „Dėl Lietuvos Respublikos viešųjų pirkimų įstatymo 92 straipsnio 13, 14 ir 15 dalių nuostatų įgyvendinimo“);

1.7.2. įrangos priežiūra ar palaikymas būtų vykdomas iš VPĮ 92 straipsnio 14 dalyje numatytame sąraše nurodytų valstybių ar teritorijų.

1.8. Tiekėjas turi laikytis šių aplinkosaugos reikalavimų:

1.8.1. mažinti popieriaus sunaudojimą, atsisakyti nebūtino dokumentų kopijavimo ir spausdinimo, rengiamą dokumentaciją, prekių perdavimo–priėmimo aktus Užsakovui pateikti tik elektroniniu formatu, visus dokumentus ir prekių perdavimo–priėmimo aktus pasirašyti elektroniniu parašu. Esant būtinybei spausdinti, naudoti perdirbtą popierių, kuris atitinka minimalius aplinkos apsaugos kriterijus, patvirtintus Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakymu Nr. D1-508 „Dėl Produktų, kurių viešiesiems pirkimams taikytini aplinkos apsaugos kriterijai, sąrašo, Aplinkos apsaugos kriterijų ir Aplinkos apsaugos kriterijų, kuriuos perkančiosios organizacijos turi taikyti pirkdamos prekes, paslaugas ar darbus, taikymo tvarkos aprašo patvirtinimo“.

1.8.2. Perkama įranga turi būti ilgaamžiška, tinkanti antriniam perdirbimui.

1.8.3. Pakuotės turi atitikti Lietuvos Respublikos pakuočių ir pakuočių atliekų tvarkymo įstatymo ir Lietuvos Respublikos aplinkos ministro 2002 m. birželio 27 d. įsakymu Nr. 348 „Dėl pakuočių ir pakuočių atliekų tvarkymo taisyklių patvirtinimo“ patvirtintų Pakuočių ir pakuočių atliekų tvarkymo taisyklių reikalavimus.

1.9. Jei iš šiose techninėse specifikacijose pateiktų duomenų būtų galima daryti prielaidą apie konkrečius technologinius procesus ar prekių ženklus, patentus, tipus, konkrečią kilmę ar gamybą, laikoma, kad jie yra tik orientaciniai ir tiekėjai gali siūlyti lygiaverčius.

2. Specialieji reikalavimai

Ugniasienės įranga:

Eil. Nr.	Parametrai	Minimalūs paslaugos reikalavimai	Siūlomos paslaugos charakteristikos/ parametrai (Pildo tiekėjas)
1.	Sprendimo architektūra ir sudedamosios dalys	Ugniasienių sprendimas turi būti sudarytas iš dviejų vienodų narių, skirtų užtikrinti perimetro kontrolę, įsibrovimų aptikimą ir prevenciją, URL filtravimą, srautų turinio kontrolę. Kiekvienas narys, t.y. kiekviena ugniasienė turi dirbti kaip nepriklausomas narys ir turi būti galima narius sujungti į aukšto patikimumo telkinį. Turi būti pateikta visa aparatinė-programinė įranga ir licencijos leidžiančios ugniasienių sprendimo narius diegti kaip nepriklausomus narius ir kaip aukšto patikimumo telkinio narius. Žemiau pateikiami reikalavimai taikomi kiekvienam nariui atskirai, t.y. reikalavimus turi tenkinti kiekvienas iš telkinio narių.	Ugniasienių sprendimas yra sudarytas iš dviejų vienodų narių, skirtų užtikrinti perimetro kontrolę, įsibrovimų aptikimą ir prevenciją, URL filtravimą, srautų turinio kontrolę. Kiekvienas narys, t.y. kiekviena ugniasienė dirba kaip nepriklausomas narys ir galima narius sujungti į aukšto patikimumo telkinį. Yra pateikta visa aparatinė-programinė įranga ir licencijos leidžiančios ugniasienių sprendimo narius diegti kaip nepriklausomus narius ir kaip aukšto patikimumo telkinio narius. Žemiau pateikiami reikalavimai taikomi kiekvienam nariui atskirai, t.y. reikalavimus tenkina kiekvienas iš telkinio narių.
2.	Sprendimo narių įrangos gamintojas, modelis, modifikacija (jei yra)	Būtina išvardinti siūlomos įrangos komponentus, jų kiekius, modelius, gamintoją ir produktų kodus. Jeigu siūloma įranga licencijuojama, būtina pateikti licencijų kodus ir trumpą funkcionalumo aprašymą, kurį kiekviena licencija suteikia.	• 2vnt. Fortinet Fortigate FG-601F 4x 25G SFP28 slots, 4 x 10GE SFP+ slots, 18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, SPU NP7 and CP9 hardware accelerated, 480GB onboard SSD storage, dual AC power supplies • 2vnt. Fortinet FC-10-0601F-950-02-36 Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)
3.	Surinkimo reikalavimai	Ugniasienių sprendimo nario įranga turi būti specializuotas	Ugniasienių sprendimo nario įranga yra specializuotas

		aparatinis-programinis įrenginys arba modulinis įrenginys su vidiniais arba išoriniais moduliais komplektuojamas paties gamintojo. Ugniasienių sprendimo narį sudarantys aparatiniai komponentai (procesoriai, atmintis ir kt.) turi būti suderinti tarpusavyje, pagaminti vieno gamintojo arba kelių gamintojų, tačiau turi būti pateiktas ugniasienės gamintojo patvirtinimas dėl komponentų tarpusavio suderinamumo. Siūloma įranga negali būti realizuota naudojant virtualizacijos platformomis paremtais sprendimais.	aparatinis-programinis įrenginys su vidiniais ir išoriniais moduliais komplektuojamas paties gamintojo. Ugniasienių sprendimo narį sudarantys aparatiniai komponentai (procesoriai, atmintis ir kt.) yra suderinti tarpusavyje, pagaminti vieno gamintojo. Siūloma įranga nėra realizuota naudojant virtualizacijos platformomis paremtais sprendimais.
4.	Įrangos suderinamumas	Siūloma ugniasienių sprendimo įranga turi būti pilnai suderinama su Perkančiosios organizacijos šiuo metu naudojamu įrašų kaupimo ir analizės įranga FortiAnalyzer. Suderinamumas turi būti paremtas Fortinet Security Fabric funkcionalumu.	Siūloma ugniasienių sprendimo įranga yra pilnai suderinama su Perkančiosios organizacijos šiuo metu naudojamu įrašų kaupimo ir analizės įranga FortiAnalyzer. Suderinamumas yra paremtas Fortinet Security Fabric funkcionalumu.
5.	Korpusas	Siūloma ugniasienių sprendimo nario įranga turi būti pritaikyta montavimui į standartinę 19 colių įrangos montavimui skirtą spintą su visais montavimui reikalingais priedais (įskaitant bet neapsiribojant tvirtinimo elementais).	Siūloma ugniasienių sprendimo nario įranga yra pritaikyta montavimui į standartinę 19 colių įrangos montavimui skirtą spintą su visais montavimui reikalingais priedais (įskaitant bet neapsiribojant tvirtinimo elementais).
6.	Maitinimo šaltiniai	Karšto keitimo tipo, pakankamos galios vidiniai maitinimo šaltiniai, kurie užtikrina aukštą patikimumą (n+1). Ugniasienių sprendimas narys turi veikti sugedus vienam maitinimo šaltiniui. Pritaikyti prijungti prie 220 – 240 V, 50 – 60 Hz kintamos srovės elektros tinklo.	Karšto keitimo tipo, pakankamos galios vidiniai maitinimo šaltiniai, kurie užtikrina aukštą patikimumą (n+1). Ugniasienių sprendimas narys veikia sugedus vienam maitinimo šaltiniui. Pritaikyti prijungti prie 220 – 240 V, 50 – 60 Hz kintamos srovės elektros tinklo.
7.	Tinklo prievadai	Prievadų kiekis ir tipas: – ne mažiau kaip 16 vnt. GE RJ45 prievadų; – ne mažiau kaip 8 vnt. GE SFP prievadų;	Prievadų kiekis ir tipas: – 16 vnt. GE RJ45 prievadų; – 8 vnt. GE SFP prievadai; – 8 vnt. GE SFP+ prievadų.

		– ne mažiau kaip 8 vnt. GE SFP+ prievadų.	
8.	Valdymo prievadai	Prievadų kiekis ir tipas: – ne mažiau kaip vienas konsolės prievadas; – ne mažiau kaip vienas valdymo prievadas skirtas įrenginio valdymui per grafinę sąsają bei komandinę eilutę. Šių prievadų skaičius turi būti papildomas, neturi būti įtrauktas į 7 punkte numatytą tinklo prievadų skaičių.	Prievadų kiekis ir tipas: – vienas konsolės prievadas; – vienas valdymo prievadas skirtas įrenginio valdymui per grafinę sąsają bei komandinę eilutę. Šių prievadų skaičius yra papildomas, nėra įtrauktas į 7 punkte numatytą tinklo prievadų skaičių.
9.	Pajungimo į aukšto patikimumo telkinį prievadai	Ne mažiau kaip 1 vnt. Šie prievadai neturi būti įtraukti į 7 punkte numatytą tinklo prievadų skaičių.	1 vnt. Šie prievadai nėra įtraukti į 7 punkte numatytą tinklo prievadų skaičių.
10.	Vidinė talpykla	Ugniasienių sprendimo narys privalo turėti ne mažiau kaip 1 SSD tipo diską su ne mažesne kaip 240 GB atmintimi.	Ugniasienių sprendimo narys turi 2vnt. SSD tipo diskų su 240 GB atmintimi.
11.	Palaikomi standartai / protokolai	Ugniasienių sprendimo narys privalo palaikyti: – kiekvienas tinklo duomenų srauto fizinis prievadas privalo palaikyti VLAN pagal 802.1Q arba lygiavertį standartą; – LACP arba lygiavertį protokolą; – bent vieną iš protokolų: Netflow, sFlow, IPFIX arba kitą lygiavertį protokolą; – 802.3ad arba lygiavertį standartą. Turi būti galimybė apjungti į vieną loginę tinklo sąsają ne mažiau kaip 4 fizines sąsajas.	Ugniasienių sprendimo narys palaiko: – kiekvienas tinklo duomenų srauto fizinis prievadas palaiko VLAN pagal 802.1Q standartą; – LACP protokolą; – protokolus: Netflow, sFlow, IPFIX; – 802.3ad standartą. Yra galimybė apjungti į vieną loginę tinklo sąsają 4 fizines sąsajas.
12.	VLAN palaikymas	Ne mažiau kaip 4000 VLAN žymių (angl. Vlan TAG) per įrenginį ir/arba prievadą.	4094 VLAN žymių (angl. Vlan TAG) per įrenginį ir/arba prievadą.
13.	Ugniasienių sprendimo nario greitaveika atliekant duomenų srautų kontrolę su aplikacijų atpažinimu ir kontrolę (ang. application control)	Ne mažiau kaip 25 Gbps.	139 Gbps

	realiame duomenų sraute, bei informacijos apie sujungimų sesijas rašymų į įvykių žurnalą.		
14.	Ugniasienių sprendimo nario greitaveika atliekant duomenų srautų kontrolę su aplikacijų atpažinimu ir kontrole, įsilaužimų prevencija (IPS) NGFW (angl. Next Generation Firewall) realiame duomenų sraute bei informacijos apie sujungimų sesijas rašymu į įvykių žurnalą.	Ne mažiau kaip 11 Gbps.	11,5 Gbps
15.	Ugniasienių sprendimo nario greitaveika atliekant duomenų srautų kontrolę su aplikacijų atpažinimu ir kontrole, įsilaužimų prevencija (IPS), kenkėjiškų kodų, antivirusine patikra realiame duomenų sraute, bei informacijos apie sujungimų sesijas rašymų į įvykių žurnalą.	Ne mažiau kaip 10 Gbps.	10,5 Gbps
16.	IPsec VPN greitaveika	Ne mažiau kaip 40 Gbps.	55 Gbps
17.	IPsec tunelių skaičius naudojant apjungimus tarp įrenginių apjungiant tinklus (angl. site to site VPN)	Ne mažiau kaip 2000.	2000
18.	IPsec tunelių skaičius naudojant vartotojų / klientų prisijungimą prie ugniasienės	Ne mažiau kaip 3000.	50000
19.	Maksimalus sesijų skaičius vienu metu	Ne mažiau kaip 6 milijonų.	8 milijonai
20.	Ugniasienių sprendimo nario vienu metu palaikomas maksimalus dešifruotų sesijų skaičius	Ne mažiau kaip 300000.	550000
21.	Suminis saugumo taisyklių skaičius per Ugniasienių sprendimo narį	Ne mažiau kaip 9000.	10000
22.	Valdymas	Turi būti: grafinė vartotojo sąsaja (GUI) per naršyklę HTTPS	Yra: grafinė vartotojo sąsaja (GUI) per naršyklę HTTPS

		protokolu, komandinė eilutė SSH protokolu. Valdymui per grafinę vartotoją sąsaja (GUI) per HTTPS neturi būti naudojama speciali gamintojo pateikiama programinė įranga arba papildomi naršyklės įskiepiai. Per valdymui skirtą grafinę vartotojo sąsają (GUI) per HTTPS turi būti galima atlikti ne mažiau kaip šiuos konfigūravimo, problemų paieškos ir analizės veiksmus: – aukšto patikimumo funkcionalumo konfigūravimas; – PBR funkcionalumo konfigūravimas; – srauto balansavimo funkcionalumo konfigūravimas; – prieigos politikų konfigūravimas; – apsaugos nuo grėsmių funkcionalumo konfigūravimas; – IPS funkcionalumo konfigūravimas; – aplikacijų valdymo funkcionalumo konfigūravimas; – URL filtravimo funkcionalumo konfigūravimas; – VPN funkcionalumo konfigūravimas; – srauto įrašų peržiūra ir paieška, filtravimas; – sisteminių įrašų peržiūra ir paieška, filtravimas; – administravimo įrašų peržiūra ir paieška, filtravimas; – VPN įrašų peržiūra ir paieška, filtravimas;	protokolu, komandinė eilutė SSH protokolu. Valdymui per grafinę vartotoją sąsaja (GUI) per HTTPS nenaudojama speciali gamintojo pateikiama programinė įranga arba papildomi naršyklės įskiepiai. Per valdymui skirtą grafinę vartotojo sąsają (GUI) per HTTPS galima atlikti šiuos konfigūravimo, problemų paieškos ir analizės veiksmus: – aukšto patikimumo funkcionalumo konfigūravimas; – PBR funkcionalumo konfigūravimas; – srauto balansavimo funkcionalumo konfigūravimas; – prieigos politikų konfigūravimas; – apsaugos nuo grėsmių funkcionalumo konfigūravimas; – IPS funkcionalumo konfigūravimas; – aplikacijų valdymo funkcionalumo konfigūravimas; – URL filtravimo funkcionalumo konfigūravimas; – VPN funkcionalumo konfigūravimas; – srauto įrašų peržiūra ir paieška, filtravimas; – sisteminių įrašų peržiūra ir paieška, filtravimas; – administravimo įrašų peržiūra ir paieška, filtravimas; – VPN įrašų peržiūra ir paieška, filtravimas;

		– maršrutizavimo įrašų peržiūra ir paieška, filtravimas; – saugos incidentų įvykių peržiūra ir paieška, filtravimas.	– maršrutizavimo įrašų peržiūra ir paieška, filtravimas; – saugos incidentų įvykių peržiūra ir paieška, filtravimas.
23.	Aukšto patikimumo savybės	Ugniasienių sprendimo narys privalo palaikyti žemiau įvardintą funkcionalumą: – nario pajungimas į aukšto patikimumo telkinį, kuris gali dirbti aktyvus – pasyvus ir aktyvus – aktyvus darbo režimais; – turi būti galimybė nurodyti, kad veikiantis ir aukštesnį prioritetą turintis narys visada būtų aktyvus telkinio narys; – automatinis konfigūracijos sinchronizavimas tarp aukšto patikimumo telkinio narių; – automatinis aktyvių sesijų sinchronizavimas tarp aukšto patikimumo telkinio narių; – turi būti galimybė iš telkinio nario stebėti ar aktyvūs nurodyti IP adresai. Sistema turi automatiškai persijungti jei nurodyti IP adresai tampa neaktyviais.	Ugniasienių sprendimo narys palaiko žemiau įvardintą funkcionalumą: – nario pajungimas į aukšto patikimumo telkinį, kuris gali dirbti aktyvus – pasyvus ir aktyvus – aktyvus darbo režimais; – yra galimybė nurodyti, kad veikiantis ir aukštesnį prioritetą turintis narys visada būtų aktyvus telkinio narys; – automatinis konfigūracijos sinchronizavimas tarp aukšto patikimumo telkinio narių; – automatinis aktyvių sesijų sinchronizavimas tarp aukšto patikimumo telkinio narių; – yra galimybė iš telkinio nario stebėti ar aktyvūs nurodyti IP adresai. Sistema automatiškai persijungia jei nurodyti IP adresai tampa neaktyviais.
24.	Įrangos virtualizavimas	Turi būti funkcionalumas, leidžiantis Ugniasienių sprendimo narį sudalinti į ne mažiau kaip 6 virtualius įrenginius.	Yra funkcionalumas, leidžiantis Ugniasienių sprendimo narį sudalinti į 10 virtualių įrenginių.
25.	Ugniasienių sprendimo nario darbo režimai	Ne mažiau kaip : – maršrutizavimo tarp skirtingų tinklų (OSI L3); – skaidrus – atliekant kontrolę tame pačiame tinkle (OSI L2); – stebėjimo – pasyviai surenkant informaciją nuo tinklo įrangos, kuri sugeba	Darbo režimai : – maršrutizavimo tarp skirtingų tinklų (OSI L3); – skaidrus – atliekant kontrolę tame pačiame tinkle (OSI L2); – stebėjimo – pasyviai surenkant informaciją nuo tinklo įrangos, kuri sugeba

		atiduoti duomenų srauto kopiją.	atiduoti duomenų srauto kopiją.
26.	Darbo režimai ir virtualizavimo funkcionalumas	Ugniasienių sprendimo narį dalinant į virtualias sistemas tos pačios fizinės sistemos apimtyje, kiekviena virtuali sistema privalo veikti kiekvienu iš darbo režimų (maršrutizavimo, skaidrus, stebėjimo), tai nustatant konfigūracijoje pasirinktinai. Kiekvienai virtualiai sistemai turi būti galimybė nustatyti darbo režimą nepriklausomai nuo to, kokiu režimu dirba kitos virtualios sistemos.	Ugniasienių sprendimo narį dalinant į virtualias sistemas tos pačios fizinės sistemos apimtyje, kiekviena virtuali sistema veikia kiekvienu iš darbo režimų (maršrutizavimo, skaidrus, stebėjimo), tai nustatant konfigūracijoje pasirinktinai. Kiekvienai virtualiai sistemai yra galimybė nustatyti darbo režimą nepriklausomai nuo to, kokiu režimu dirba kitos virtualios sistemos.
27.	Maršrutizavimas	Ugniasienių sprendimo narys privalo palaikyti statinius bei dinaminius maršrutizavimo protokolus bei politika pagrįstą maršrutizavimą (angl. Policy based routing).	Ugniasienių sprendimo narys palaiko statinius bei dinaminius maršrutizavimo protokolus bei politika pagrįstą maršrutizavimą (angl. Policy based routing).
28.	Maršrutizavimas	Ugniasienių sprendimo narys privalo palaikyti statinių maršrutų tikrinimo mechanizmą, kuomet maršrutas panaikinamas iš maršrutizavimo lentelės, jeigu nepasiekiami vienas ar keli aprašyti IP adresai.	Ugniasienių sprendimo narys palaiko statinių maršrutų tikrinimo mechanizmą, kuomet maršrutas panaikinamas iš maršrutizavimo lentelės, jeigu nepasiekiami vienas ar keli aprašyti IP adresai.
29.	PBR (angl. Policy based routing) funkcionalumas	Ugniasienių sprendimo narys privalo palaikyti politika pagrįstą maršrutizavimą (angl. Policy based routing) atsižvelgiant į šaltinio/paskirties zoną arba sąsają, siuntėjo, gavėjo IP adresą.	Ugniasienių sprendimo narys palaiko politika pagrįstą maršrutizavimą (angl. Policy based routing) atsižvelgiant į šaltinio/paskirties zoną arba sąsają, siuntėjo, gavėjo IP adresą.
30.	Dinaminio maršrutizavimo protokolai	Ugniasienių sprendimo narys privalo palaikyti žemiau įvardintus arba lygiaverčius protokolus: – BGP; – OSFP v2 ir v3; – RIP v2.	Ugniasienių sprendimo narys palaiko žemiau protokolus: BGP; OSFP v2 ir v3; RIP v2.
31.	BGP funkcionalumas	Ugniasienių sprendimo narys privalo turėti grakštaus BGP perkrovimo (graceful restart) funkcionalumą.	Ugniasienių sprendimo narys turi grakštaus BGP perkrovimo (graceful restart) funkcionalumą.
32.	BGP konfigūracijos palaikymas	Ugniasienių sprendimo narys privalo palaikyti šiuos BGP protokolo gebėjimus: – maksimalų išmokstamų maršrutų skaičiaus ribojimą per kaimyną;	Ugniasienių sprendimo narys palaiko šiuos BGP protokolo gebėjimus: – maksimalų išmokstamų maršrutų skaičiaus ribojimą per kaimyną;

		– BGP kaimynų grupavimą; – filtravimą gaunamiems ir išsiunčiamiems maršrutams; – Local Preference; – MED; – AS prepend; – Route-reflector funkcionalumą; – maršrutų stabilumo vertinimą (prefix dampening); – BGP BFD; – BGP community; – Next hop vertės keitimą; – Soft session reset.	– BGP kaimynų grupavimą; – filtravimą gaunamiems ir išsiunčiamiems maršrutams; – Local Preference; – MED; – AS prepend; – Route-reflector funkcionalumą; – maršrutų stabilumo vertinimą (prefix dampening); – BGP BFD; – BGP community; – Next hop vertės keitimą; – Soft session reset.
33.	OSPF funkcionalumas	Ugniasienių sprendimo narys privalo turėti grakštaus OSPF perkrovimo (graceful restart) funkcionalumą.	Ugniasienių sprendimo narys turi grakštaus OSPF perkrovimo (graceful restart) funkcionalumą.
34.	BFD palaikymas	Ugniasienių sprendimo narys privalo palaikyti BFD (bidirectional forwarding detection) protokolą.	Ugniasienių sprendimo narys palaiko BFD (bidirectional forwarding detection) protokolą.
35.	IPv6 palaikymas	Ugniasienių sprendimo narys privalo palaikyti IPv6 protokolą.	Ugniasienių sprendimo narys palaiko IPv6 protokolą.
36.	Jumbo paketai	Ugniasienių sprendimo narys turi palaikyti Jumbo paketus.	Ugniasienių sprendimo narys palaiko Jumbo paketus.
37.	Adresų transliavimo funkcionalumas	Ugniasienių sprendimo narys privalo palaikyti žemiau įvardintą arba lygiavertį funkcionalumą: – NAT64; – Statinis adresų transliavimas; – Dinaminis adresų transliavimas keičiant prievadus (PAT).	Ugniasienių sprendimo narys palaiko žemiau įvardintą funkcionalumą: – NAT64; – Statinis adresų transliavimas; – Dinaminis adresų transliavimas keičiant prievadus (PAT).
38.	Integracija su SNMP (Simple Network Management Protocol) įrenginio būsenos stebėjimui	Privalo palaikyti SNMP protokolo 2 ir 3 versijas.	Palaiko SNMP protokolo 2 ir 3 versijas
39.	Suderinamumas su Syslog	Ugniasienių sprendimo narys turi būti suderinamas su Syslog standartu.	Ugniasienių sprendimo narys yra suderinamas su Syslog standartu.
40.	Centralizuoto valdymo palaikymas	Privalo būti galimybė Ugniasienių sprendimo narį valdyti iš centrinio, valdymui dedikuoto, sprendimo.	Yra galimybė Ugniasienių sprendimo narį valdyti iš centrinio, valdymui dedikuoto, sprendimo.

41.	Įvykių žurnalų (event log) palaikymas	Ugniasienių sprendimo narys privalo palaikyti žemiau įvardintus įvykių žurnalus: – sisteminiai; – administravimo; – VPN; – naudotojų autentifikavimo; – maršrutizavimo; – saugos incidentų įvykiai.	Ugniasienių sprendimo narys palaiko žemiau įvardintus įvykių žurnalus: – sisteminiai; – administravimo; – VPN; – naudotojų autentifikavimo; – maršrutizavimo; – saugos incidentų įvykiai.
42.	Įvykių žurnalų kaupimas	Ugniasienių sprendimo narys privalo leisti kaupti įvykių žurnalus įrenginio talpykloje ir siųsti į nuotolinį – centralizuotą įvykių žurnalų kaupimui skirtą sprendimą.	Ugniasienių sprendimo narys leidžia kaupti įvykių žurnalus įrenginio talpykloje ir gali siųsti į nuotolinį – centralizuotą įvykių žurnalų kaupimui skirtą sprendimą.
43.	Diagnostikos priemonės	Privalomas srauto / paketų nuo konkretaus interfeiso „įsirašymas“ (packet capture) diagnostikos tikslais su papildomu filtrų (pageidaujami įsirašymo parametrai) užsidėjimu.	Yra srauto / paketų nuo konkretaus interfeiso „įsirašymas“ (packet capture) diagnostikos tikslais su papildomu filtrų (pageidaujami įsirašymo parametrai) užsidėjimu.
44.	Nutolusių naudotojų duomenų bazių palaikymas	Ugniasienių sprendimo narys privalo palaikyti žemiau įvardintas arba lygiavertes duomenų bazes: – LDAP; – RADIUS; – TACACS+; – dviejų lygių (two-factor) autentifikacija.	Ugniasienių sprendimo narys palaiko žemiau įvardintas duomenų bazes: – LDAP; – RADIUS; – TACACS+; – dviejų lygių (two-factor) autentifikacija.
45.	Prieigos teisių valdymas	Ugniasienių sprendimo narys privalo: – leisti suteikti prieigos teises tik naudotojams, kurių tapatybė yra patvirtinta; – leisti suteikti prieigos teises naudotojams ir/arba naudotojų grupėms; – leisti nustatyti naudotojų tapatybę, neprašydamas suvesti naudotojo vardo ir slaptažodžio, o pasinaudodamas jau esamomis tinklo paslaugomis, pvz., Active directory arba programinės įrangos (agento) pagalba;	Ugniasienių sprendimo narys gali: – leidžia suteikti prieigos teises tik naudotojams, kurių tapatybė yra patvirtinta; – leidžia suteikti prieigos teises naudotojams ir/arba naudotojų grupėms; – leidžia nustatyti naudotojų tapatybę, neprašydamas suvesti naudotojo vardo ir slaptažodžio, o pasinaudodamas jau esamomis tinklo paslaugomis, pvz., Active directory arba

		– leisti sukurti naudotoją – administratorių, kuris turėtų tik read-only teises (galimybė matyti visą konfigūraciją, bet keisti nieko negalima); – leisti detaliai/individualiai apibrėžti kiekvieno fizinio ir/ar virtualaus naudotojo/administratoriaus teises: • teisė keisti sisteminius įrenginio nustatymus; • teisė kurti, keisti saugumo taisykles; • teisė kurti, keisti taisyklių objektus; • teisė konfigūruoti saugumo patikrų nustatymus; • teisė peržiūrėti įvykių žurnalus; • teisė peržiūrėti ataskaitas; • teisė generuoti ataskaitas.	programinės įrangos (agento) pagalba; – leidžia sukurti naudotoją – administratorių, kuris turėtų tik read-only teises (galimybė matyti visą konfigūraciją, bet keisti nieko negalima); – leidžia detaliai/individualiai apibrėžti kiekvieno fizinio ir/ar virtualaus naudotojo/administratoriaus teises: • teisė keisti sisteminius įrenginio nustatymus; • teisė kurti, keisti saugumo taisykles; • teisė kurti, keisti taisyklių objektus; • teisė konfigūruoti saugumo patikrų nustatymus; • teisė peržiūrėti įvykių žurnalus; • teisė peržiūrėti ataskaitas; • teisė generuoti ataskaitas.
46.	Autorizacijos integracija (single sign on)	Ugniasienių sprendimo narys privalo turėti integracijas su žemiau įvardintomis arba lygiavertėmis sistemomis: – Windows AD; – Microsoft Exchange server; – Citrix Terminal Server Agent; – RADIUS; – 802.1x.	Ugniasienių sprendimo narys turi integracijas su žemiau įvardintomis sistemomis: – Windows AD; – Microsoft Exchange server; – Citrix Terminal Server Agent; – RADIUS; – 802.1x.
47.	SSL šifruoto srauto inspekcija	Ugniasienių sprendimo narys turi dešifruoti ir tikrinti įeinantį ir išeinantį SSL duomenų srautą. Ugniasienių sprendimo narys privalo palaikyti SSL šifruoto srauto inspektavimą į narį įkeliant reikiamus sertifikatus.	Ugniasienių sprendimo narys gali dešifruoti ir tikrinti įeinantį ir išeinantį SSL duomenų srautą. Ugniasienių sprendimo narys palaiko SSL šifruoto srauto inspektavimą į narį įkeliant reikiamus sertifikatus.

		Privalo būti galimybė nurodyti kuris duomenų srautas turi būti dešifruojamas.	Yra galimybė nurodyti kuris duomenų srautas turi būti dešifruojamas.
48.	DoS apsauga	Ugniasienių sprendimo narys privalo leisti riboti sesijų arba paketų per sekundę skaičius jų šaltiniui arba adresatui.	Ugniasienių sprendimo narys leidžia riboti sesijų arba paketų per sekundę skaičius jų šaltiniui arba adresatui.
49.	Apsauga nuo grėsmių	Ugniasienių sprendimo narys turi saugoti nuo atakų, piktybinių kodų (pvz. virusai, šnipinėjimo programos), stabdyti konfidencialios informacijos perdavimą (pvz.: pagal raktinius žodžius, pagal IT politiką), tikrinti perduodamą srautą nuo virusų. Turi būti galimybė naudoti gamintojo pateikiamus dinamiškai atnaujinamus kenksmingų IP adresų sąrašus.	Ugniasienių sprendimo narys saugo nuo atakų, piktybinių kodų (pvz. virusai, šnipinėjimo programos), stabdo konfidencialios informacijos perdavimą (pvz.: pagal raktinius žodžius, pagal IT politiką), tikrina perduodamą srautą nuo virusų. Yra galimybė naudoti gamintojo pateikiamus dinamiškai atnaujinamus kenksmingų IP adresų sąrašus.
50.	Protokolų anomalijos	Ugniasienių sprendimo narys privalo palaikyti žemiau įvardintą funkcionalumą: – protokolų anomalijų aptikimas; – protokolų anomalijų, nuosavo „parašo“ susikūrimas ir įkėlimas į sistemą.	Ugniasienių sprendimo narys palaiko žemiau įvardintą funkcionalumą: – protokolų anomalijų aptikimas; – protokolų anomalijų, nuosavo „parašo“ susikūrimas ir įkėlimas į sistemą.
51.	IPS funkcionalumas	Ugniasienių sprendimo narys turi turėti galimybę palaikyti žemiau įvardintą funkcionalumą: - įsilaužimų / pažeidžiamumų (IPS) aprašų duomenų bazės palaikymas pačiame įrenginyje ir nuolatinis tos bazės atnaujinimas. - turi būti galimybė užblokuoti atakuojantį IP adresą. - leisti nustačius grėsmę automatiškai įrašyti paketus, susijusius su grėsme.	Ugniasienių sprendimo narys turi galimybę palaikyti žemiau įvardintą funkcionalumą: - įsilaužimų / pažeidžiamumų (IPS) aprašų duomenų bazės palaikymas pačiame įrenginyje ir nuolatinis tos bazės atnaujinimas. - yra galimybė užblokuoti atakuojantį IP adresą. - leidžia nustačius grėsmę automatiškai įrašyti paketus, susijusius su grėsme.
52.	Protokolų anomalijos	Ugniasienių sprendimo narys privalo palaikyti žemiau įvardintą funkcionalumą: - protokolų anomalijų aptikimas; - protokolų anomalijų, nuosavo „parašo“ susikūrimas ir įkėlimas į sistemą.	Ugniasienių sprendimo narys palaiko žemiau įvardintą funkcionalumą: - protokolų anomalijų aptikimas; - protokolų anomalijų, nuosavo „parašo“ susikūrimas ir įkėlimas į sistemą.

53.	Aplikacijų valdymas	Ugniasienių sprendimo narys privalo palaikyti: – aplikacijų identifikavimą ir kontrolę. Turi identifikuoti ne mažiau kaip 3000 aplikacijų (Tos pačios programos skirtingos versijos skaičiuojamos kaip viena programa). Aplikacijų aprašai pateikiami nemokamai (arba įskaičiuoti į pasiūlymo kainą) netrumpesniam kaip ugniasienių sprendimo nario įrangos garantinio aptarnavimo laikotarpiui; – aplikacijų atpažinimo nuosavo aprašo susikūrimą ir įkėlimą į sistemą.	Ugniasienių sprendimo narys palaiko: – aplikacijų identifikavimą ir kontrolę. Identifikuoja ne mažiau kaip 4300 aplikacijų (Tos pačios programos skirtingos versijos skaičiuojamos kaip viena programa). (Aplikacijų kiekis nuolat didėja ir jį galima stebėti čia - https://www.fortiguard.com/appcontrol). Aplikacijų aprašai pateikiami nemokamai ugniasienių sprendimo nario įrangos garantinio aptarnavimo laikotarpiui; – aplikacijų atpažinimo nuosavo aprašo susikūrimą ir įkėlimą į sistemą.
54.	URL filtravimas	Ugniasienių sprendimo narys privalo palaikyti: – prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę (URL filtravimas); – nuosavų draudžiamų URL sąrašų kūrimas; – URL, IP adresų, domenų vardų, kurie bus naudojami saugumo politikose, importavimas iš išorinio failo.	Ugniasienių sprendimo narys palaiko: – prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę (URL filtravimas); – nuosavų draudžiamų URL sąrašų kūrimas; – URL, IP adresų, domenų vardų, kurie bus naudojami saugumo politikose, importavimas iš išorinio failo.
55.	Sesijų laiko kontrolė	Turi būti galimybė kiekvienai aplikacijai nustatyti individualų laiką, po kurio neaktyvi sesija yra uždaroma.	Yra galimybė kiekvienai aplikacijai nustatyti individualų laiką, po kurio neaktyvi sesija yra uždaroma.
56.	Duomenų srautų kontrolės taisyklės	Kuriant duomenų srautų kontrolės taisyklės privalo būti galimybė nurodyti siuntėjo IP adresą ar potinklį, gavėją IP adresą ar potinklį, siuntėjo šalį, gavėjo šalį servisą/prievadą, programą, taikytinas apsaugos priemones, vartotoją, vartotojų grupę.	Kuriant duomenų srautų kontrolės taisykles yra galimybė nurodyti siuntėjo IP adresą ar potinklį, gavėją IP adresą ar potinklį, siuntėjo šalį, gavėjo šalį servisą/prievadą, programą, taikytinas apsaugos priemones, vartotoją, vartotojų grupę.

		Privalo būti galimybė skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones.	Yra galimybė skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones.
57.	Duomenų srautų kontrolės taisyklių naudojimo stebėjimas	Ugniasienių sprendimo narys privalo rodyti taisyklių žymas: taisyklės panaudojimo skaičius (angl. hit count).	Ugniasienių sprendimo narys rodo taisyklių žymas: taisyklės panaudojimo skaičius (angl. hit count).
58.	VPN funkcionalumas	Ugniasienių sprendimo narys privalo turėti žemiau įvardintą VPN funkcionalumą: – leisti redaguoti SSL VPN portalą; – leisti naudotis SSL VPN WEB naršyklės pagalba (be papildomos aplikacijos / agento); – nuotolinio prisijungimo naudotojo VPN klientas turi mokėti dirbti IPSec ir SSL protokolais; – nuotolinio prisijungimo naudotojo SSL VPN klientas (programinė įranga) privalo būti to paties gamintojo kaip ir siūlomų ugniasienių sprendimo įrenginių gamintojas arba skirtingų gamintojų, suderinamas bendram darbui. Jei siūlomas skirtingo gamintojo VPN klientas (programinė įranga) nei ugniasienių sprendimo įrenginių gamintojas, turi būti pateikti abiejų gamintojų patvirtinimai, kad siūlomas sprendimas yra visiškai suderinamas bendram darbui su ugniasienių sprendimu; – nuotolinio prisijungimo VPN klientas turi palaikyti galimybę naudoti skaitmeninius sertifikatus tapatybės nustatymui.	Ugniasienių sprendimo narys turi žemiau įvardintą VPN funkcionalumą: – leidžia redaguoti SSL VPN portalą; – leidžia naudotis SSL VPN WEB naršyklės pagalba (be papildomos aplikacijos / agento); – nuotolinio prisijungimo naudotojo VPN klientas moka dirbti IPSec ir SSL protokolais; – nuotolinio prisijungimo naudotojo SSL VPN klientas (programinė įranga) yra to paties gamintojo kaip ir siūlomų ugniasienių sprendimo įrenginių gamintojas. – nuotolinio prisijungimo VPN klientas palaiko galimybę naudoti skaitmeninius sertifikatus tapatybės nustatymui.
59.	IPSec šifravimo algoritmai	Ugniasienių sprendimo narys privalo palaikyti žemiau įvardintus arba lygiaverčius IPSec šifravimo algoritmus:	Ugniasienių sprendimo narys palaiko žemiau įvardintus IPSec šifravimo algoritmus: – AES128;

		– AES128; – AES256.	– AES256.
60.	IPSec maišos algoritmai	Ugniasienių sprendimo narys privalo palaikyti žemiau įvardintus arba lygiaverčius IPSec maišos algoritmus: – SHA-256; – SHA-512.	Ugniasienių sprendimo narys palaiko žemiau įvardintus IPSec maišos algoritmus: SHA-256; SHA-512.
61.	Srauto ribojimas	Ugniasienių sprendimo narys privalo leisti riboti srautą ir taikyti QoS per taisyklę (policy).	Ugniasienių sprendimo narys leidžia riboti srautą ir taikyti QoS per taisyklę (policy).
62.	Aprašų, programinės įrangos atnaujinimas	Ugniasienių sprendimo narys privalo galėti automatiškai, reguliariai, nustatytu laiku atsisiųsti ir aktyvuoti aplikacijų, pažeidžiamumų, virusų, kenkėjiškų kodų aprašus, URL filtravimo duomenų bazę arba gauti informaciją realiu laiku iš gamintojo serverių / puslapio. Ugniasienių sprendimo narys privalo galėti atsisiųsti programinės įrangos atnaujinimas iš gamintojo puslapio.	Ugniasienių sprendimo narys gali automatiškai, reguliariai, nustatytu laiku atsisiųsti ir aktyvuoti aplikacijų, pažeidžiamumų, virusų, kenkėjiškų kodų aprašus, URL filtravimo duomenų bazę ir gauti informaciją realiu laiku iš gamintojo serverių / puslapio. Ugniasienių sprendimo narys gali atsisiųsti programinės įrangos atnaujinimus iš gamintojo puslapio.

Ugniasienės diegimo ir palaikymo paslaugos:

1. Diegimo paslaugos.

Eil. nr.	Parametrai	Reikalavimai paslaugai
1.	Projekto valdymas	Tiekėjas atsakingas už projekto valdymą. Perkančioji organizacija pateiks turimą dokumentaciją ir prisijungimus. Tiekėjas įsipareigoja teikti projekto eigos savaitines ataskaitas.
2.	Projektavimas	Turi būti atlikta esamos situacijos analizė: - migravimo ir testavimo plano paruošimas. Migravimas turi būti vykdomas etapais – migruojant po vieną virtualią sistemą.
3.	Montavimas	Turi būti atlikta: - ugniasienių transportavimas į užsakovo duomenų centrą; - esamos įrangos demontavimas; - naujos įrangos sumontavimas.
4.	Migravimas	Turi būti atliktas konfigūracijos perkėlimas ir ryšių perjungimas iš šiuo metu Perkančiosios organizacijos naudojamo ugniasienių Fortigate 400D telkinio, kuriame šiuo metu sukonfigūruota ~400 saugumo politikų. Turi būti atlikti, įskaitant, bet neapsiribojant šie konfigūravimo darbai: - IP adresų, SSH, SNMP, NTP, SYSLOG konfigūravimas; - IP adresų/servisų objektų konfigūravimas; - prieigos taisyklių konfigūravimas; - saugumo profilių konfigūravimas;

		- NAT konfigūravimas; - site-to-site IPsec VPN konfigūravimas; - nuotolinės prieigos darbuotojams konfigūravimas; - RADIUS, LDAP serverių IP konfigūravimas; - lokalių administratorių paskyrų ir paskyrų profilių kūrimas; - statinės ir dinaminės maršrutizacijos konfigūravimas; - MLAG/LAG agreguotų sąsajų konfigūravimas; - VLAN konfigūravimas; - prievadų konfigūravimas; - virtualių sistemų konfigūravimas; - programinės įrangos atnaujinimas ir saugos aprašų duomenų bazių atnaujinimas iki naujausios gamintojo siūlomos versijos; - aukšto patikimumo telkinio konfigūravimas; - ugniasienių integravimas su užsakovo turima tinklo įranga.
5.	Testavimas	Turi būti atlikta: - ugniasienių aukšto patikimumo testavimas; - 4 punkte išvardintų konfigūravimo darbų rezultatų testavimas; - 2 sav. sistemos stebėjimas po migracijos ir problemų šalinimas.
6.	Dokumentacija	Pabaigus visus šioje lentelėje nurodytus darbus (tiek projektavimo, tiek sprendimo diegimo) turi būti pateikta atliktų darbų dokumentacija ir pateiktos infrastruktūros schemos, techninės bei programinės įrangos nustatymai: – susijusios IT infrastruktūros esamos fizinės ir loginės schemos; – įdiegtų sprendimų principinio veikimo schemos; – įdiegtų sprendimų įrangos konfigūracijos; – sukonfigūruoti kredencialai; – įdiegtų sprendimų įrangos dokumentacija.

2. Palaikymo paslaugos.

Eil. Nr.	Parametrai	Minimalūs paslaugos reikalavimai
1.	Palaikymų paslaugų tipas	siūlomų ugniasienių gamintojo suteikiamos palaikymo paslaugos
2.	Garantijos ir licencijų palaikymo paslaugos	Įsigyjamos ugniasienės įrangos palaikymo paslaugos, kurios turi apimti: - programinės įrangos (angl. hardware) palaikymą 24 x 7 režimu (24 val. per parą, 7 dienos per savaitę); - įrangos programinių atnaujinimų (angl. firmware & general updates) palaikymą 24 x 7 režimu (24 val. per parą, 7 dienos per savaitę); - pagalbą ir konsultacijas kreipiantis telefonu, el. paštu, internetiniuose pokalbiuose (angl. online chat) ar internetiniame portale 24 x 7 režimu (24 val. per parą, 7 dienos per savaitę); - gedimo atveju, išankstinį įrangos pristatymą (angl. advanced hardware replacement (NBD));

		- ugniasienės gamintojo suteikiamas FortiGuard paslaugas: o aplikacijų kontrolę (angl. Application Control); o įsibrovimų prevenciją ir aplikacijų kontrolę (angl. - IPS and Application Control); o antivirusinę kontrolę (angl. – AntiVirus); o Web filtravimą (angl. – Web Filtering); o el. pašto skenavimą (angl. – Email Filtering); o mobilių įrenginių apsaugą nuo kenkėjiško kodo (angl. Mobile Malware); o kenksmingų bylų emuliavio debesyje paslaugą (angl. Sandbox).
3.	Aprašų, programinės įrangos atnaujinimas	Privalo galėti automatiškai, reguliariai, nustatytu laiku atsisiųsti ir aktyvuoti aplikacijų, pažeidžiamumų, virusų, kenkėjiškų kodų aprašus, URL filtravimo duomenų bazę arba gauti informaciją realiu laiku iš gamintojo serverių / puslapio. Ugniasienių sprendimo narys privalo galėti atsisiųsti programinės įrangos atnaujinimas iš gamintojo puslapio.
4.	Garantiniai įsipareigojimai, techninis aptarnavimas.	Visiems techninės ir programinės įrangos komponentams, turi būti suteikta ne trumpesnė nei 36 mėn. gamintojo garantija, skaičiuojant nuo įrangos priėmimo-perdavimo akto pasirašymo dienos. Gamintojo garantuojamas nemokamas garantinis aptarnavimas bei visų atnaujinimų tiekimas garantiniu laikotarpiu (aplikacijų kontrolės, virusų, piktybinių programų, pažeidžiamumų, įsilaužimo aprašų, URL filtravimo duomenų bazių ir kt. pagal I pirkimo dalyje aprašytus techninėje specifikacijoje aprašytus reikalavimus). Programinės įrangos palaikymas (teisė gauti klaidų pataisymus, taip pat naujesnes programinės įrangos versijas), Teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) savaitės dienomis visą parą (paslaugos tipas 24x7) (telefonu ar kitomis elektroninėmis priemonėmis). Gedimo atveju gamintojas turi užtikrinti įšankstinį įrangos pristatymą (angl. advanced hardware replacement (NBD)). Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos lietuvių arba anglų kalbomis.
5.	Palaikymo laikotarpis	36 mėn. nuo įrangos įdiegimo dienos.

2022 m. lapkričio d. sutarties
Nr. LRVK- 3 priedas

Uždaroji akcinė bendrovė, J. Jasinskio g. 16A, LT-03163 Vilnius, tel. (8 5) 252 6060, el. p. info@bluebridge.lt, duomenys apie įmonę kaupiami ir saugomi VĮ Registrų centras juridinių asmenų registre, 301489547, LT100003708514

Lietuvos Respublikos Vyriausybės kanceliarijai
(Adresatas (perkančioji organizacija))

PASIŪLYMAS
DĖL TINKLO UGNIASIENĖS ĮRANGOS PIRKIMO
2022-10-13 Nr. PSL221005EDR1-01
(Data)
Vilnius
(Sudarymo vieta)

Tiekėjo pavadinimas */Jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių pavadinimai/*	Blue Bridge MSP, UAB
Tiekėjo adresas */Jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių adresai/*	J. Jasinskio g. 16A, LT-03163 Vilnius
Asmens, pasirašiusio pasiūlymą kvalifikuotu elektroniniu parašu, vardas, pavardė, pareigos	Eglė Drungilaitė, pardavimų koordinatorė
Telefono numeris	+37052526060
Fakso numeris	+37052526069
El. pašto adresas	info@bluebridge.lt

Pildoma, jei tiekėjas ketina pasitelkti subtiekėją:

Subtiekėjo (-ų) pavadinimas (-ai)*	
Subtiekėjo (-ų) adresas (-ai)	
Įsipareigojimų dalis (procentais), kuriai ketinama pasitelkti subtiekėją (-us)	

1. Šiuo pasiūlymu pažymime, kad sutinkame su visomis pirkimo sąlygomis, nustatytomis:

1) supaprastinto atviro konkurso skelbime, paskelbtame Viešųjų pirkimų įstatymo nustatyta tvarka CVP IS interneto adresu: https://pirkimai.eviesiejipirkimai.lt;

2) kituose pirkimo dokumentuose (jų paaiškinimuose, papildymuose).

2. Pasirašydamas CVP IS priemonėmis pateiktą pasiūlymą kvalifikuotu elektroniniu parašu, patvirtinu, kad dokumentų skaitmeninės kopijos ir elektroninėmis priemonėmis pateikti duomenys yra tikri.

3. Pateikdamas pasiūlymą sutinku, kad vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymo 86 straipsnio 9 dalimi, laimėjimo atveju, CVP IS būtų paskelbti: pasiūlymas, sudaryta pirkimo sutartis ir jos pakeitimai (jei tokie bus).

4. Pasiūlymas galioja iki 2022 m. lapkričio 30 d.

Siūlomos prekės ir paslaugos visiškai atitinka pirkimo dokumentuose nurodytus reikalavimus: **pridedame užpildytą techninės specifikacijos (pirkimo sąlygų 2 priedo) formą ir siūlomų prekių dokumentus, patvirtinančius, kad Tiekėjas yra gamintojo oficialus ir sertifikuotas atstovas, įgaliotas parduoti Užsakovui reikalingas prekes.**

Siūlome *šias prekes ir paslaugas*:

Eil. Nr.	Prekės ir paslaugos	Kaina Eur be PVM
1.	Tinklo ugniasienės įranga	25 416,00
2.	Įrangos diegimo ir 36 mėn. palaikymo paslaugos	54 934,00
3.	**Iš viso:**	80 350,00
4.	**21% PVM**	16 873,50
5.	**Bendra pasiūlymo kaina Eur su PVM**	97 223,50

*Į bendrą pasiūlymo kainą turi būti įskaičiuoti visi su sutarties vykdymu susiję tiekėjo mokesčiai bei kitos išlaidos, įskaitant ir sąskaitų teikimo per „E-sąskaita“ sistemą mokestį.

Tais atvejais, kai pagal galiojančius teisės aktus tiekėjui nereikia mokėti PVM, jis nurodo priežastis, dėl kurių PVM nemokamas:_____

Kartu su pasiūlymu pateikiami šie dokumentai:

Eil. Nr.	Pateiktų dokumentų pavadinimas	Dokumento puslapių skaičius	Ar dokumentas konfidencialus (Taip/Ne)
1.	EBVPD	16	Ne
2.	Įgaliojimas	1	Ne
3.	Techninė specifikacija	17	Ne
4.	Gamintojo raštas	1	Ne
5.	Produktų kodai_Konfidencialu	1	Taip

Pastaba. Tiekėjui nenurodžius, kokia informacija yra konfidenciali, laikoma, kad konfidencialios informacijos pasiūlyme nėra.

Pardavimų koordinatorė		Eglė Drungilaitė
(Tiekėjo arba jo įgalioto asmens pareigų pavadinimas*)	(Parašas*)	(Vardas ir pavardė*)

*Pastaba. Jei visas pasiūlymas pasirašomas kvalifikuotu elektroniniu parašu, šio dokumento atskirai pasirašyti neprivaloma.

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Blue Bridge MSP, UAB 301489547, J. Jasinskio g. 16A, LT-03163 Vilnius Lietuvos Respublikos Vyriausybės kanceliarija 188604574, Vilniaus m. sav., Vilniaus m., Gedimino pr. 11
Dokumento pavadinimas (antraštė)	Tinklo ugniasienės įranga
Dokumento registracijos data ir numeris	2022-11-09 Nr. LRVK-138/22
Dokumento gavimo data ir dokumento gavimo registracijos numeris	–
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Suderinimas
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	
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	
Parašo paskirtis	
Parašą sukūrusio asmens vardas, pavardė ir pareigos	
Sertifikatas išduotas	

DETALŪS METADUOMENYS	
Parašo sukūrimo data ir laikas	
Parašo formatas	
Laiko žymoje nurodytas laikas	
Informacija apie sertifikavimo paslaugų teikėją	
Sertifikato galiojimo laikas	
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Alminas Mačiulis, Vyriausybės kanclerio pavaduotojas, Lietuvos Respublikos Vyriausybės kanceliarija
Sertifikatas išduotas	ALMINAS MAČIULIS, Lietuvos Respublikos Vyriausybės kanceliarija LT
Parašo sukūrimo data ir laikas	2022-11-08 14:27:48 (GMTZ)
Parašo formatas	XAdES-EPES
Laiko žymoje nurodytas laikas	–
Informacija apie sertifikavimo paslaugų teikėją	ADIC CA-A, Asmens dokumentu israsymo centras prie LR VRM LT
Sertifikato galiojimo laikas	2021-10-19 13:28:41 – 2024-10-18 13:28:41
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Gintautas Bazys, -
Sertifikatas išduotas	BAZYS,GINTAUTAS,PNOLT-37802151045 LT
Parašo sukūrimo data ir laikas	2022-11-08 18:03:50 (GMT+02:00)
Parašo formatas	XAdES-T
Laiko žymoje nurodytas laikas	2022-11-08 18:04:03 (GMT+02:00)
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016, AS Sertifitseerimiskeskus EE
Sertifikato galiojimo laikas	2021-06-09 08:47:33 – 2024-06-09 08:47:33
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	"Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "RCSC IssuingCA, VI Registru centras - i.k. 124110246 LT" išduotą sertifikatą "Dokumentų, informacijos ir veiklos procesų valdymo informacinė sistema (DIVIS), Lietuvos Respublikos Vyriausybės kanceliarija, į.k. 188604574 LT", sertifikatas galioja nuo 2021-12-20 11:00:45 iki 2024-12-19 11:00:45
Pagrindinio dokumento priedų skaičius	2
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	Dokumentų informacijos ir veiklos procesų valdymo informacinė sistema DIVIS, versija 3.5.51
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja (2022-11-09 08:43:02)
Paieškos nuoroda	–
Papildomi metaduomenys	Nuorašą suformavo 2022-11-09 08:43:04 Dokumentų informacijos ir veiklos procesų valdymo informacinė sistema DIVIS