ANTIVIRUSINĖS PROGRAMINĖS ĮRANGOS VIEŠOJO PIRKIMO SUTARTIS

2021 m. kovo d. Nr. (1.10-04-2E)-22-
Vilnius

Valstybinė mokesčių inspekcija prie Lietuvos Respublikos finansų ministerijos (toliau — UŽSAKOVAS), atstovaujama viršininkės Editos Janušienės, veikiančios pagal Valstybinės mokesčių inspekcijos prie Lietuvos Respublikos finansų ministerijos nuostatus, ir UAB „NBCS“ (toliau — TIEKĖJAS), atstovaujama generalinio direktoriaus Artiom Maslov, veikiančio pagal bendrovės įstatus, (toliau abi vadinamos — ŠALYS, kiekviena atskirai toliau vadinama — ŠALIS), atsižvelgdamos į viešojo pirkimo „Antivirusinės programinės įrangos viešasis pirkimas“ (pirkimo Nr. 532206), atlikto supaprastinto atviro konkurso būdu (toliau — PIRKIMAS), rezultatus, sudarė šią sutartį (toliau — SUTARTIS).

PIRKIMAS įvyko vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymu ir Lietuvos Respublikos civiliniu kodeksu. PIRKIME TIEKĖJUI pateikti PIRKIMO dokumentai ir TIEKĖJO pateiktas pasiūlymas toliau yra vadinami „KONKURSO DOKUMENTAIS“. Jeigu SUTARTIS nenustato kitaip, SUTARTYJE naudojamos sąvokos reiškia tą patį, ką ir KONKURSO DOKUMENTUOSE naudojamos sąvokos.

1. SUTARTIES DALYKAS

1.1. SUTARTIES dalykas - programinė įranga ir licencijos skirtos kompiuterizuotų darbo vietų apsaugai nuo kompiuterinių virusų, nepageidaujamų elektroninių laiškų ir kitų žalingų veiksnių, iš Interneto, elektroninio pašto ir kitų duomenų perdavimo kanalų (toliau – PREKĖS), taip pat teisė gauti programinės įrangos gamintojo palaikymą (toliau − PREKIŲ TIEKIMAS). PREKIŲ TIEKIMAS detalizuotas SUTARTYJE.

1.2. Visa nauda, kurią TIEKĖJAS suteiks UŽSAKOVUI SUTARTIES galiojimo metu, vykdydamas SUTARTIES nuostatas, toliau vadinama - PREKIŲ TIEKIMO rezultatu.

1.3. PREKIŲ TIEKIMĄ atlieka TIEKĖJAS UŽSAKOVUI.

1.4. SUTARTYJE nustatyti PREKIŲ TIEKIMO atlikimui ir TIEKĖJUI privalomi reikalavimai, visi KONKURSO DOKUMENTUOSE, su PREKIŲ TIEKIMO atlikimu susiję, numatyti TIEKĖJUI kaip privalomi po SUTARTIES sudarymo, tačiau neįkelti į SUTARTIES tekstą reikalavimai bei kituose dokumentuose, į kuriuos daro nuorodą KONKURSO DOKUMENTAI, nustatyti PREKIŲ TIEKIMO atlikimui ir TIEKĖJUI kaip privalomi po SUTARTIES sudarymo reikalavimai, toliau SUTARTYJE vadinami REIKALAVIMAIS.

1.5. PREKIŲ TIEKIMAS turi būti vykdomas pagal REIKALAVIMUS. TIEKĖJAS įsipareigoja atlikti PREKIŲ TIEKIMĄ pagal REIKALAVIMUS.

1.6. Įsigaliojus naujiems Lietuvos Respublikos teisės aktams, susijusiems su PREKIŲ TIEKIMO atlikimu, TIEKĖJAS privalo vykdyti tokių teisės aktų nuostatas nuo jų įsigaliojimo datos. Kiekviena REIKALAVIMŲ nuostata, neatitinkanti įsigaliojusio naujojo Lietuvos Respublikos teisės akto, susijusio su PREKIŲ TIEKIMO atlikimu, nuo tokio naujojo teisės akto įsigaliojimo datos netaikoma, o vietoj jos taikoma įsigaliojusio naujojo Lietuvos Respublikos teisės akto, susijusio su PREKIŲ TIEKIMO atlikimu, nuostata.

2. KAINA IR ATSISKAITYMAS

2.1. UŽSAKOVAS TIEKĖJUI avanso nemoka, t. y. iš anksto su TIEKĖJU neatsiskaito.

2.2. PREKIŲ TIEKIMO kaina – yra 106500,00 (Vienas šimtas šeši tūkstančiai penki šimtai eurų 00 ct) be PVM, 128865,00 (Vienas šimtas dvidešimt aštuoni tūkstančiai aštuoni šimtai šešiasdešimt penki eurai 00 ct) su PVM.

2.3. PREKIŲ TIEKIMO kainos detalizavimas:

Eil. Nr.	Pavadinimas	Gamintojo PREKĖS pavadinimas, PREKĖS kodas	Kiekis, vnt.	Vieneto kaina, Eur be PVM	Vieneto kaina, Eur su PVM
1.	Programinės įrangos su 3300 vnt. licencijų pristatymas ir diegimas UŽSAKOVO infrastruktūroje, teisė gauti 3 metų trukmės gamintojo programinės įrangos palaikymą pagal techniniuose reikalavimuose nurodytus reikalavimus.	F-Secure Business Suite Premium FCUPSR3NVXFIN	1	106500,00	128865,00
2.	UŽSAKOVO darbuotojo apmokymas eksploatuoti ir administruoti siūlomą programinę įrangą gamintojo mokymo centre.	-	2	0,00	0,00

2.4. TIEKĖJAS PVM sąskaitą - faktūrą turi pateikti per informacinę sistemą „E. sąskaita“. Elektroninės paslaugos „E. sąskaita“ svetainė pasiekiama adresu www.esaskaita.eu.

2.5. UŽSAKOVAS atsiskaito su TIEKĖJU per 30 dienų, nuo dienos, kai tinkamai įvykdomas PREKIŲ TIEKIMAS ir UŽSAKOVAS patvirtina PVM sąskaitą faktūrą „E.sąskaita“ informacinėje sistemoje.

2.6. Atsiskaitymas įvykdomas UŽSAKOVUI atitinkamą sumą pervedus į SUTARTYJE nurodytą TIEKĖJO sąskaitą.

2.7. Į PREKIŲ TIEKIMO kainą turi būti įskaičiuotos visos TIEKĖJO išlaidos ir mokesčiai, būtini, kad būtų visiškai įvykdyta SUTARTIS.

2.8. PREKIŲ TIEKIMO rezultato naudojimas negali reikalauti iš UŽSAKOVO jokių papildomų išlaidų.

2.9. Atsiskaitymai pagal SUTARTĮ vykdomi eurais.

2.10. PREKIŲ TIEKIMO įkainiai dėl kainų lygio pasikeitimo ir pasikeitusių mokesčių neperskaičiuojami, išskyrus žemiau nurodytą atvejį.

2.11. SUTARTIES kainodaros taisyklė – fiksuotas įkainis (be PVM). SUTARTYJE nustatytų įkainių su PVM peržiūra atliekama, kai pasikeičia pridėtinės vertės mokestis (PVM). SUTARTIES galiojimo metu joje nustatyti PREKIŲ TIEKIMO įkainiai, turi būti koreguojami, taikant naują pasikeitusį PVM dydį.

3. PREKIŲ TIEKIMO ATLIKIMAS

3.1. Visi UŽSAKOVO numatyti reikalavimai (visos sąlygos), susiję su PREKIŲ tiekimu, SUTARTYJE tampa TIEKĖJO įsipareigojimais.

3.2. PREKIŲ TIEKIMAS vykdomas po SUTARTIES pasirašymo.

3.3. PREKĖS turės būti pristatytos ir įdiegtos per 14 kalendorinių dienų. Pristatymo adresas Vasario 16-osios g. 14 Vilnius. Programinė įranga diegiama visuose UŽSAKOVO padaliniuose esančioje kompiuterizuotose darbo vietose, visoje Lietuvos Respublikos teritorijoje.

3.4. UŽSAKOVO darbuotojų apmokymas eksploatuoti ir administruoti siūlomą programinę įrangą turi būti atliktas per 60 kalendorinių dienų nuo SUTARTIES pasirašymo dienos.

3.5. UŽSAKOVO nuosavybės teisė PREKĖMS ar PREKIŲ daliai (dalims), kurios pagal Civilinį kodeksą yra nuosavybės teisių objektas, atsiranda nuo to momento, kai TIEKĖJAS PREKES ar PREKIŲ dalį (dalis) perduoda UŽSAKOVUI.

3.6. TIEKĖJO atstovai PREKIŲ TIEKIMO klausimais su UŽSAKOVO atstovais bendrauja lietuvių kalba.

3.7. PREKIŲ TIEKIMO kokybė turi atitikti REIKALAVIMUS ir Civilinio kodekso nuostatas.

3.8. UŽSAKOVO atsakingi asmenys už SUTARTIES vykdymą – UŽSAKOVO Informacinių išteklių valdymo departamento Informacinių išteklių administravimo skyriaus vyriausiasis specialistas Nerijus Mačiulevičius, el. p. Nerijus.Maciulevicius@vmi.lt, tel. (8 5) 2687 991 ir UŽSAKOVO Informacinių išteklių valdymo departamento Informacinių išteklių administravimo skyriaus vedėjas Raimondas Puodžiūnas, el. p. Raimondas.Puodziunas@vmi.lt, tel. (8 5) 2687 860. Apie pasikeitusius atsakingus asmenis TIEKĖJAS bus informuojamas raštu.

4. ŠALIŲ ATSAKOMYBĖ

4.1. ŠALYS privalo susilaikyti nuo bet kokių veiksmų, kurie galėtų pakenkti kitai ŠALIAI.

4.2. Jei TIEKĖJAS neįvykdo arba netinkamai įvykdo SUTARTYJE numatytus įsipareigojimus, UŽSAKOVAS turi teisę pareikalauti atlyginti SUTARTIES sąlygų nevykdymu ar netinkamu vykdymu jam padarytus tiesioginius nuostolius, bet ne didesne nei SUTARTIES verte, išskyrus Civilinio kodekso 6.252 straipsnio 1 dalyje įtvirtintas išimtis ir pagal Civilinį kodeksą galimus regreso atvejus.

4.3. Jei TIEKĖJAS vėluoja atlikti PREKIŲ TIEKIMO dalį „Programinės įrangos su 3300 vnt. licencijų pristatymas ir diegimas UŽSAKOVO infrastruktūroje, teisė gauti 3 metų trukmės gamintojo programinės įrangos palaikymą“ daugiau kaip 14 kalendorinių dienų, jam taikoma 10 procentų nuo PREKIŲ TIEKIMO dalies kainos dydžio bauda.

4.4. Jei TIEKĖJAS vėluoja atlikti PREKIŲ TIEKIMO dalį „UŽSAKOVO darbuotojo apmokymas eksploatuoti ir administruoti siūlomą programinę įrangą“ daugiau kaip 30 kalendorinių dienų, jam taikoma 5 procentų nuo PREKIŲ TIEKIMO dalies kainos dydžio bauda.

4.5. Už UŽSAKOVO vėlavimą atsiskaityti su TIEKĖJU numatomi delspinigiai — 0,06 procento nuo vėluojamos apmokėti sumos, už kiekvieną pavėluotą dieną, bet ne daugiau kaip 5 procentai nuo bendros SUTARTIES vertės. UŽSAKOVUI delspinigiai neskaičiuojami, jeigu vėlavimas atsiranda dėl netinkamo UŽSAKOVO finansavimo.

4.6. Jeigu naudojimosi PREKIŲ TIEKIMO rezultatu metu paaiškės, kad UŽSAKOVUI atitenkanti TIEKĖJO perduota susijusi su PREKIŲ TIEKIMU dokumentacija yra neišsami, ir jos nepakanka, kad įvykdytų kokį nors iš SUTARTYJE numatytų PREKIŲ TIEKIMO tikslų, su tuo susijusius UŽSAKOVO nuostolius padengs TIEKĖJAS.

4.7. Nutraukus SUTARTĮ 5.5.2 punkte nurodytu pagrindu, TIEKĖJAS per 5 (penkias) darbo dienas nuo SUTARTIES nutraukimo dienos sumoka UŽSAKOVUI 10 procentų nuo SUTARTIES vertės dydžio baudą ir TIEKĖJAS įtraukiamas į nepatikimų tiekėjų sąrašą.

5. SUTARTIES GALIOJIMAS, PAKEITIMAS IR NUTRAUKIMAS

5.1. SUTARTIS įsigalioja nuo jos pasirašymo momento ir galioja iki visiško TIEKĖJO ir UŽSAKOVO įsipareigojimų pagal SUTARTĮ įvykdymo momento.

5.2. SUTARTIS sudaroma 36 mėn. laikotarpiui.

5.3. UŽSAKOVAS turi teisę nutraukti SUTARTĮ, jeigu TIEKĖJAS SUTARTIES galiojimo laikotarpiu pagal galiojančius teisės aktus praranda teisę užsiimti ūkine - komercine ar kitokia, būtina PREKIŲ TIEKIMO atlikimui, veikla.

5.4. Jeigu TIEKĖJAS netinkamai vykdo SUTARTĮ, UŽSAKOVAS gali ją nutraukti įspėjęs TIEKĖJĄ prieš 10 kalendorinių dienų.

5.5. SUTARTIS gali būti nutraukta anksčiau nurodyto termino:

5.5.1. ŠALIŲ rašytiniu susitarimu;

5.5.2. UŽSAKOVAS gali nutraukti SUTARTĮ, prieš 10 kalendorinių dienų įspėjęs raštu TIEKĖJĄ, jeigu jis nevykdo sutartinių įsipareigojimų ar netinkamai juos įvykdo ir tai yra esminis SUTARTIES pažeidimas. Nustatydamas esminį SUTARTIES pažeidimą UŽSAKOVAS privalo vadovautis Lietuvos Respublikos civilinio kodekso 6.217 straipsnio nuostatomis;

5.5.3. ŠALIS gali nutraukti SUTARTĮ, jeigu kita ŠALIS netinkamai vykdo SUTARTYJE numatytus įsipareigojimus ir jeigu prieš tai ją įspėjus raštu, per rašte nurodytą protingą terminą neištaisė dėl SUTARTIES nevykdymo ar netinkamo vykdymo susidariusių trūkumų.

5.6. UŽSAKOVAS gali vienašališkai nutraukti SUTARTĮ Viešųjų pirkimų įstatymo 90 straipsnio 1 dalyje nurodytais pagrindais.

5.7. Jeigu TIEKĖJAS savo iniciatyva anksčiau laiko nori nutraukti SUTARTĮ, TIEKĖJAS gali ją nutraukti tik raštu įspėjęs UŽSAKOVĄ prieš 10 kalendorinių dienų. Šiuo atveju TIEKĖJAS per 5 darbo dienas nuo SUTARTIES nutraukimo dienos sumoka UŽSAKOVUI 10 procentų nuo SUTARTIES vertės dydžio baudą, TIEKĖJAS taip pat įsipareigoja per 5 darbo dienas nuo UŽSAKOVO reikalavimo kompensuoti UŽSAKOVUI visus tiesioginius nuostolius, atsiradusius dėl tokio SUTARTIES nutraukimo, kurių nepadengia bauda.

5.8. Visi SUTARTIES pakeitimai, papildymai, priedai galioja, jeigu jie yra sudaryti raštu ir patvirtinti abiejų ŠALIŲ įgaliotų atstovų parašais. Visi SUTARTIES pakeitimai, papildymai ir priedai tampa sudėtinėmis ir neatskiriamomis SUTARTIES dalimis.

5.9. SUTARTIES sąlygos SUTARTIES galiojimo laikotarpiu negali būti keičiamos, išskyrus

Viešųjų pirkimų įstatymo 89 straipsnyje numatytus atvejus.

5.10.UŽSAKOVAS pasilieka teisę atsisakyti viso PREKIŲ TIEKIMO ar PREKIŲ TIEKIMO dalies pirkimo, jeigu jis neturės pakankamo, nuo jo nepriklausančio finansavimo (UŽSAKOVAS yra iš Lietuvos Respublikos biudžeto finansuojama, Lietuvos Respublikos mokesčių administratoriaus funkcijas atliekanti įstaiga), arba PREKIŲ TIEKIMO ar PREKIŲ TIEKIMO dalies pirkimo nereikės vykdant mokesčių administratoriaus funkcijas, arba dėl kitų priežasčių. Šiuo atveju jokios sankcijos, numatytos SUTARTYJE, UŽSAKOVUI netaikomos. Tokio atsisakymo atveju UŽSAKOVAS apmoka TIEKĖJUI už iki atsisakymo faktiškai įvykdytą pagal SUTARTĮ PREKIŲ TIEKIMO dalį. Tokiu atsisakymu gali būti nepranešimas TIEKĖJUI apie prekių ir (ar) paslaugų tiekimo pradžią (užsakymo nepateikimas).

6. NENUGALIMOS JĖGOS APLINKYBĖS (FORCE MAJEURE)

6.1. Nė viena iš SUTARTIES ŠALIŲ neatsako už prisiimtų įsipareigojimų visišką ar dalinį neįvykdymą, jeigu ji įrodo, kad įsipareigojimų neįvykdė dėl nenugalimos jėgos aplinkybių (Force Majeure).

6.2. ŠALIS, kuri dėl nenugalimos jėgos aplinkybių negali įvykdyti savo įsipareigojimų, privalo nedelsdama, bet ne vėliau kaip per 5 dienas nuo aplinkybių atsiradimo ar paaiškėjimo, raštu informuoti apie tai kitą ŠALĮ. Pranešime išdėstyti faktai turi būti patvirtinti kompetentingos valdžios institucijos. Jeigu nenugalimos jėgos aplinkybės užsitęsia ilgiau kaip tris mėnesius, ŠALYS tarpusavio susitarimu gali nutraukti SUTARTĮ.

6.3. Nenugalimos jėgos aplinkybėmis yra laikomos aplinkybės, apibrėžtos Civilinio kodekso 6.212 straipsnyje ir Atleidimo nuo atsakomybės esant nenugalimos jėgos aplinkybėms taisyklėse, patvirtintose Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840.

7. BAIGIAMOSIOS NUOSTATOS

7.1. SUTARTIES punktų pavadinimai nustatomosios galios neturi - jų tikslas yra tik palengvinti SUTARTIES nuostatų paiešką.

7.2. SUTARTIS sudaroma Civilinio kodekso pagrindu. Visiems ginčams, kilusiems dėl SUTARTIES vykdymo, spręsti taikomi Lietuvos Respublikos norminiai teisės aktai

7.3. Visi ginčai, kylantys dėl SUTARTIES tarp ŠALIŲ, sprendžiami ŠALIŲ tarpusavio sutarimu, o nesutarus, Lietuvos Respublikos teisme.

7.4. SUTARTIS sudaryta 2 egzemplioriais, turinčiais vienodą juridinę galią. Kiekvienai iš ŠALIŲ įteikiamas vienas SUTARTIES egzempliorius.

7.5. SUTARTIS turi priedą PREKIŲ TIEKIMO TECHNINĖ SPECIFIKACIJA, kuris yra neatskiriama SUTARTIES dalis.

UŽSAKOVAS:
Valstybinė mokesčių inspekcija prie Lietuvos Respublikos finansų ministerijos
Vasario 16-sios g. 14, LT-01514 Vilnius
Telefonas: (8 5) 268 7800
Kodas: 188659752
Atsiskaitomoji sąskaita:
LT68 7300 0100 7573 5365
Swedbank AB

Viršininkė

Edita Janušienė

TIEKĖJAS:
UAB „NBCS“
Adresas: J. Kazlausko g. 21, 08314 Vilnius
Telefonas: 8 5 2764563
Kodas: 301817848
el. p. info@nbcs.lt
Atsiskaitomoji sąskaita:
LT417044060008319438
AB „SEB“ Bankas

Generalinis direktorius

Artiom Maslov

1 priedas

PREKIŲ TIEKIMO TECHNINĖ SPECIFIKACIJA

Techniniai reikalavimai perkamai programinei įrangai:

Visos lentelėje nurodytos techninės savybės turi būti realizuotos vieno (to paties) gamintojo programinėje įrangoje.

Eil. nr.	**Reikalavimai**
Reikalavimai antivirusinei programinės įrangos sistemai kompiuterinėms darbo vietoms (stacionarai ir nešiojami kompiuteriai) ir tarnybinėms stotims (rinkmenų ir el. pašto tarnybinės stotys):	
1.	Automatinė apsauga realiu laiku nuo virusų, kirminų, šnipinėjimo programų, „trojos arklių“, „rootkits“, „riskware“, „web“ ir el.pašto srautui stacionariems ir nešiojamiems kompiuteriams, tarnybinėms stotims.
2.	Realiu laiku skenavimas išorinių įrenginių, vietinių diskų ir tinklo diskų nuo žalingų programų.
3.	Turi būti integruotas apsaugos mechanizmas nuo prieigos prie kompiuterio išnaudojant programinės įrangos pažeidžiamumus.
4.	Sistema turėtų naudoti užklausomis paremtą žalingų programų aprašų reputacijos tikrinimą (panaudojant debesų kompiuterijos technologiją).
5.	Sprendimas turėtų naudoti hešuotą talpą žalingų programų laikymui.
6.	Sprendimas darbo vietoms ir tarnybinėms stotims turi turėti ne mažiau dviejų skenavimo variklių virusų ir šnipinėjimo programų aptikimui ir turi būti integruota vienoje platformoje.
7.	Sprendimas turi galėti automatiškai pakeisti saugumo politikos nustatymus (kaip, kad pavyzdžiui ugniasienės profilis) remiantis lokacija (vidiniame tinkle arba išorėje) mobiliems įrenginiams (nešiojamiems kompiuteriams).
8.	Žalingų programų signatūrų ir skenavimo variklio atnaujinimas kompiuterinėse darbo vietose turi galėti vykti tarp kompiuterinių darbo vietų esančių tame pačiame lokaliame kompiuteriniame tinkle, tam, kad nebūtų apkraunamas interneto ryšys. Tokio atnaujinimo tipui turi nereikėti diegti tarpinės atnaujinimų tarnybinės stoties ar vietinės atnaujinimų tarnybinės stoties. Taip pat sistema turėtų gebėti identifikuoti ir nesiųsti atnaujinimų infrastruktūroje nenaudojamoms programinės įrangos versijoms darbo vietose (pralaidumo sunaudojimui mažinimo tikslais).
9.	Sprendimas turi užtikrinti karantino galimybes, kuris veiktų tokiu principu, kad atjungia kompiuterinę darbo vietą turinčią neatnaujintų aprašų duomenų bazę nuo organizacijos tinklo aplinkos iki tol kol aprašų duomenų bazė bus atnaujinta ir kompiuteris nuskenuotas nuo žalingos programinės įrangos.
10.	Turi būti apsauga nuo neatpažintų atakų, kurios bando pasinaudoti sistemos pakeitimais, internetinės naršyklės „užgrobimu“ ir kodo injekcijomis.
11.	Turi skenuoti POP3, SMTP ir IMAP4 srautą realiu laiku nuo žalingų programų.
12.	Turi skenuoti HTTP srautą nuo virusų prieš duomenų perdavimą į internetinę naršyklę.
13.	Palaikomos kalbos: anglų, prancūzų, vokiečių, lenkų, rusų.
14.	Turi būti automatinis atnaujinimas su atsarginiais atnaujinimo kanalais t.y. šalia pagrindinio atnaujinimo kanalo turi būti papildomai nemažiau kaip du alternatyvūs atnaujinimų pateikimo kanalai.
15.	Automatinis žalingų programų šalinimas, turi būti konfigūruojama administratoriaus (leisti/neleisti).
16.	Rankinis ir pagal nustatytą planą sistemos skenavimas, turi būti konfigūruojamas administratoriaus arba pačio vartotojo jei administratorius tokią galimybę suteikė.
17.	Virusų ir šnipinėjimo (angl. Spyware) skenavimo istorija turi būti atvaizduojama tiek kompiuterinėje darbo vietoje, tiek valdymo konsolėje, taip pat turi būti galimybė panaikinti statistiką.

18.	Turi būti renkama statistika apie skenuotus failus, leidžiamas programas, išvalytus failus ir blokuotas programas.
19.	Skenavimo variklis turi veikti aprašu ir euristika paremtomis technologijomis.
20.	„Rootkit“ žalingos programos aptikimas ir šalinimas.
21.	Žalingų programų aptikimas remiantis jų elgsena.
22.	Turi būti integruota interneto naršymo apsaugos funkcija, kuri turi identifikuoti žalingus internetinius puslapius ir juos blokuoti.
23.	Sprendimas turi turėti internetinių tinklalapių reputacijos nustatymo technologiją mobiliems įrenginiams, tokiems kaip nešiojamieji kompiuteriai siekiant apsaugoti šiuos įrenginius nuo infekcijos plintančios iš tinklalapių su prasta reputacija.
24.	Naršymo apsauga turi saugoti internetinę naršyklę ir jos įskiepius nuo žinomų pažeidžiamumų.
25.	Internetinio turinio kontrolė turi leisti blokuoti svetaines su nepriimtinu turiniu.
26.	Turi būti atliekamas visų aktyvių procesų atminties intervalų skenavimas.
27.	Turi būti integruota asmeninė ugniasienės, apsaugos nuo įsiveržimo sistema technologija kompiuterinėms darbo vietoms.
28.	Ugniasienės taisyklės ir profiliai turi būti konfigūruojami remiantis IP adresu, prievado numeriu, pasiekiama DNS tarnybine stotimi, protokolo tipu, naudojamu tinklo potinkliu ir kryptimi.
29.	Turi būti galimybė kontroliuoti prieigą prie tinklo remiantis aplikacija.
30.	Galimybė registruoti įvykius ir įspėti apie juos atsiradus kai pažeidžiama apsaugos nuo įsiveržimo sistemos taisyklė.
31.	Turi būtu galimybė administratoriui blokuoti DNS užklausas iš „hosto“ domenams su žalinga reputacija.
32.	Centralizuota aplikacijų kontrolė ir prisijungimo į internetą šiomis aplikacijomis blokavimo galimybės.
33.	Turi būti integruota išorinių įrenginių kontrolės funkcionalumas.
34.	Turi būti galimybė automatiškai šalinti konfliktuojančią programinę įrangą saugumo programinės įrangos diegimo metu.
35.	Turi būti galimybė iš vienos centrinės konsolės atlikti sistemos nustatymus.
36.	Diegimo platforma darbo vietos apsaugai: Windows 10 32-bit ir 64-bit; Windows 8 ir 8.1 32 bit ir 64 bit; Windows 7 32-bit ir 64-bit; Windows Vista 32-bit ir 64-bit (turi būti pateikta versija galinti palaikyti šią OS); Windows XP 32-bit SP3 (esant poreikiui turi būti pateikta versija diegimui šioje OS); Windows XP Home Edition SP2/SP3 (esant poreikiui turi būti pateikta versija diegimui šioje OS); Windows XP Professional Edition SP2/SP3 (esant poreikiui turi būti pateikta versija diegimui šioje OS); macOS versija 10.12 "Sierra"; OS X version 10.11 "El Capitan“; OS X version 10.10 "Yosemite"; CentOS 6 32-bit ir 64-bit; Debian 7.0 -ų.9 32-bit ir 64-bit; Red Hat Enterprise Linux6 32-bit ir 64-bitUbuntu 12.04.(1-5) 14.04.(1-5).
37.	Diegimo platforma darbo vietos apsaugai: Windows 10 32-bit ir 64-bit; Windows 8 ir 8.1 32 bit ir 64 bit; Windows 7 32-bit ir 64-bit; macOS versija 10.12 "Sierra"; OS X version 10.11 "El Capitan“; OS X version 10.10 "Yosemite"; CentOS 6 32-bit ir 64-bit; Debian 7.0 -ų.9 32-bit ir 64-bit; Red Hat Enterprise Linux6 32-bit ir 64-bitUbuntu 12.04.(1-5) 14.04.(1-5). Diegimo platforma serverio apsaugai: Microsoft Windows Server 2008; Microsoft Windows Server 2008 R2; Microsoft Small Business Server 2008; Microsoft Small Business Server 2011 (Standard edition); Microsoft Small Business Server 2011 (Essentials); Microsoft Windows Server 2012; Microsoft Windows Server 2012 Essentials; Microsoft Windows Server 2012 R2; Microsoft Windows Server 2012 R2 Essentials; Microsoft Windows Server 2012 R2 Foundation; Microsoft Windows Server 2016 Standard; Microsoft Windows Server 2016 Essentials; Microsoft Windows Server 2016 Datacenter. Microsoft Sharepoint (2010, 2013, 2016), EMC CAVA serveriams, SUSE Linux Enterprise Server 11 SP1/SP3 32-bit ir 64-bit; SUSE Linux Enterprise Server 12 (64-bit); Terminalinės tarnybinės stotys (Microsoft Windows Terminal/RDP Services (viršuje minėtoms Windows Server versijoms); Citrix XenApp 5.0; Citrix XenApp 6.0; Citrix XenApp 6.5; Citrix XenApp

	7.5 ir 7.6.
Reikalavimai Microsoft Exchange Antivirus ir Antispam programinei įrangai:	
38.	Turi būti naudojami nemažiau, kaip du skenavimo varikliai.
39.	Turi saugoti įeinantį, išeinantį ir vidinį el. pašto srautą, bei MS Exchange viešus katalogus nuo kenkėjiškų programų, bei atlikti turinio ir priedėlių skenavimą.
40.	Skenavimo variklis turi būti atnaujinamas automatiškai.
41.	Turi būti naudojama „grayware“ skenavimo technologija leidžianti aptikti žalingą programinę įrangą, kaip „spyware“, „adware“, „dialers“, „joke“, nuotolinio prisijungimo įrankius ir kitas nepageidaujamas programas ir rinkmenas.
42.	Euristinis skenavimas nežinomų Windows ir macro virusų aptikimui.
43.	Rekursinis skenavimas ARJ, BZ2, CAB, GZ, JAR, LZH, MSI,RAR, TAR, TGZ ir ZIP archyvuotų failų.
44.	Slaptažodžiu apsaugotus archyvus turi būti galima laikyti ir taikyti saugumo politiką, kaip nesaugiems.
45.	Įtartini ir nesaugūs priedėliai gali būti pašalinti iš el. pašto.
46.	Galimybė el.laiškus filtruoti remiantis raktažodžiais el.laiško pavadinimo (angl. Subject) eilutėje ir turinyje.
47.	Virusai turi būti neutralizuoti prieš jiems patenkant į tinklą ir išplintant į darbo vietas ar tarnybines stotis.
48.	Turi būti realiu laiku skenuojamas gaunamos ir siunčiamos el.pašto žinutės.
49.	Technologija turi būti nematoma vartotojui, tai reiškia, kad el. laiškais ir priedėliais galima apsikeisti tik juos nuskenavus.
50.	Turi būti galimybė iš vienos centrinės valdymo konsolės atlikti sistemos nustatymus.
51.	Efektyviai kovai su nepageidaujamu paštu turi būti naudojamos šios technologijos: prisijungimo analizė (DNS, MX įrašo, SPF, gavėjo reputacijos tikrinimas); kontekstinė, leksinė ir paveikslėlio analizė, "spam" filtravimas į abi puses (įeinančiam/išeinančiam srautams), batv (bounce adress tag verification), nepageidaujamas el.paštas turi būti aptinkamas įvairiose kalbose, įskaitant sunkiai analizuojamus kelių baitų simbolius, tokių kalbų, kaip kinų ar japonų.
52.	Turi būti integruotas el.pašto karantino valdymo galimybė leidžianti paskirtiems vartotojams „išlaisvinti“, inicijuoti pakartotinį skenavimą ar ištrinti karantinuotą el.paštą ir priedėlius.
Reikalavimai antivirus prieigos kontrolės vartų programinei įrangai:	
53.	Sistema turi stebėti interneto naršymo ir el. pašto srautą (HTTP, FTP, SMTP, POP) prieš patenkant jam į vidinį tinklą
54.	POP3 srauto virusų skenavimas siekiant apsaugoti tinklą nuo virusų atakų per vartotojų asmenines webmail pašto prieigas.
55.	Sistema turi galėti integruotis su trečių šalių tarpinėmis tarnybinėmis stotimis per ICAP protokolą.
56.	Turinio filtravimo galimybės, kurios turi būti nustatomos pagal failų tipą, dydį, pavadinimą.
57.	ActiveX ir Java koduotės skenavimo/blokavimo galimybės.
58.	Turi būti galimybė įspėjimo tekstus (pav. rinkmena užkrėsta virusu) keisti ir naudoti UTF-8 koduotės simbolius.
59.	Sistema turi aptikti virusus orientuotus į Windows, DOS, Microsoft Office, VBS, Linux ir kitas aplinkas.
60.	Virusų aprašų bazė turi būti atnaujinama automatiškai.
61.	Skenavimo variklis turi palaikyti ir skenuoti įvarius archyvavimo formatus (ZIP, ARJ, LZH, CAB, RAR, TAR, GZIP, BZIP2).
62.	Galimybė aptikti nepageidaujamą el. paštą (brukalą) prieigos vartuose (prieš jiems patenkant į el. pašto serverį) tiek SMTP tiek POP srautams, todėl sistema turi turėti integruotą nepageidaujamų laiškų aptikimo variklį, galimybę naudoti RBL (real time black list), SURBL (SPAM URL Realtime Black List) technologijas.

63.	Prieigos vartų programinė įranga turėtų diegtis šioje aplinkoje: 32-bit: CentOS 5/6, Debian 7.4, Red Hat Enterprise Linux 5/6, Ubuntu 12.04.4; 64-bit(x86_64): CentOS 5/6, Debian 7.4, Red Hat Enterprise Linux 5/6, Ubuntu 12.04.4.
Reikalavimai centralizuotam administravimui:	
64.	Valdymo konsolė turi turėti galimybę importuoti Active Directory domeno struktūrą ir taisykles.
65.	Antivirusinė programinė įranga kompiuteriams (stacionarams ir nešiojamiems) ir tarnybinėms stotims, antivirusinė programinė įranga Microsoft Exchange pašto tarnybiniai stočiai ir antivirusinė prieigos vartų programinė įranga turi būti valdoma iš vienos centralizuoto valdymo konsolės.
66.	Konsolė turi pateikti automatiškai ataskaitas apie naudojamas aplikacijas administratoriui.
67.	Ataskaitas turi būti galima peržiūrėti internetinėje naršyklėje ir taip pat turi būti galima eksportuoti į kitus formatus.
68.	Galimybė administratoriui blokuoti aplikacijas.
69.	Galimybė konfigūruoti sistemų skenavimo tvarkaraštį.
70.	Galimybė nuotolinių būdu valdyti karantiną.
71.	Galimybė įtraukti į baltą sąrašą (angl. Whitelisting) tinklalapius remiantis URL reputacijos analize.
72.	Žalingos programos atakos metu, sprendimas turi turėti galimybę informuoti apie incidentą valdymo konsolėje, el. paštu ir įtraukti įvykį į registrą.
73.	Atnaujinimas programinės įrangos aprašų duomenų bazių darbo vietoms/tarnybinėms stotims turi būti galimas per centrine tarnybinę stotį ir su galimybe nustatyti atnaujinimo tarpines tarnybines stotis.
74.	Ataskaitų servisas (paremtas web naršykle) turi suteikti informacijos apie žalingo kodo aktyvumą tinkle, atliktus veiksmus, atakuotus vartotojus, infekuotus vartotojus, informuoti apie saugumo pažeidžiamumus, statistiką apie atnaujinimo situaciją aprašų duomenų bazės, TOP10 ir pan.
75.	Galimybė sukurti taisyklių "medį" detalesniems nustatymams.
76.	Galimybė peržiūrėti nustatymus/savybes domenui arba "hostui".
77.	Galimybė importuoti naujus "hostus" į specifinius domenus.
78.	Automatinis „hostų“ suradimas iš Windows domeno.
79.	„Hostų“ ar domenų perkėlimo galimybė naudojant "cut" ir "paste" operacijas.
80.	Valdymo konsolė turėtų turėti galimybę būti vieninteliu atnaujinimo tašku ir galėti valdyti programinės įrangos pagerinimo procesus, taip pat nešiojamiems kompiuteriams turi būti užtikrinami kiti atsinaujinimo šaltiniai jei toks kompiuteris yra ne tinkle tam tikru laiko periodu.
81.	Nustatymų išplatinimas vartotojams ir galimybė paslėpti juos nuo vartotojo.
82.	Galimybė daryti išimtis pasirinktų plėtinių skenavimui (kad būtų neskenuojami).
83.	Galimybė daryti skenavimo išimtis remiantis pakaitos simboliais (angl. Wildcards).
84.	Galimybė pasirinkti ar tinklo diskai turi būti įtraukti į realaus laiko skenavimą.
85.	Galimybė pasirinkti ar sekimo slapukai (angl. Tracking cookies) turi būti skenuojami.
86.	Galimybė pasirinkti ar skenuoti suspaustus ir archyvuotus priedėlius rankiniame arba pagal grafiką nustatytame skenavime.
87.	Galimybė nustatyti patikimus HTTP puslapius, kurie nebus skenuojami web srauto skenavimo metu.
88.	Įspėjimo žinučių siuntimas skirtingais el. pašto adresais priklausomai nuo įspėjimo tipo.
89.	Galimybė nustatyti draudimą vartotojui diegti/išdiegti saugumo programinę įrangą iš kompiuterinės darbo vietos.
90.	Galimybė apibrėžti kaip dažnai apsaugomas komponentas bandys kreiptis į centrinę

	tarnybinę stotį.
91.	Galimybė nustatyti, kaip dažnai tarnybinė stotis bando siųsti naujus periodinius informacijos biuletenius (pav. statistika) versijas.
92.	Galimybė gauti statistiką apie naujausios infekcijos datą, naujausios infekcijos pavadinimą, naujausios infekcijos objektą, naujausios infekcijos metu apsaugos sistemos atliktus veiksmus, bendrą infekcijų skaičių.
93.	Galimybė gauti statistiką apie naujausią ataką prieš ugniasienę, naujausios atakos šaltinį, naujausios atakos servisą, statistiką apie pasirinkto laikotarpio atakas.
94.	Galimybė gauti glaustą informaciją apie saugumo sistemos komponentus sudiegtus kompiuteryje ir informaciją apie versijas.
95.	Centrinis valdymas turi palaikyti tiek MS Windows, tiek Linux platformas administruojamų ir saugumo įrenginių.
96.	Galimybė matyti paskutinės konfigūracijos laiko štampą.
97.	Galimybė rūšiuoti prisijungusius saugumo komponentus (angl. host) ir rodyti neprisijungusius.
98.	Galimybė matyti saugumo komponento WINS savybes, IP, DNS ir operacines sistemos informaciją.
99.	Diegimas tinkle į saugumo komponentą remiantis IP adresu arba saugumo komponento pavadinimu.
100.	Galimybė sukurti MSI instaliacinį failą diegimo tikslams.
101.	Galimybė centralizuoto diegimo tikslais sukurti rinkmeną paremtą paruoštuko (angl. script) metodu.
102.	Galimybė blokuoti kompiuterių su sena virusų aprašų duomenų baze prieigą prie interneto.
103.	Pavienių žalingų programų aprašų atnaujinimo galimybė.
104.	Vietinis atnaujinimo aprašų išdalinimas tinklo kompiuteriams su galimybe atnaujinti pavienius aprašus.
105.	Galimybė valdyti linux sistemų klientus iš centrinės valdymo konsolės.
Operacinės sistemos Windows ir trečių šalių programinės įrangos atnaujinimų (pataisų) valdymo funkcionalumo reikalavimai:	
106.	Turi būti integruotas programinės įrangos atnaujinimų (pataisų) valdymo funkcionalumas leidžiantis iš siūlomo sprendimo centralizuotos valdymo konsolės atnaujinti tiek Windows operacinės sistemos, tiek trečių šalių programinės įrangos atnaujinimus.
107.	Atnaujinimas turi būti galima atlikti tiek pagal nustatomą atnaujinimų politiką, tiek rankiniu būdu.
108.	Turi būti galimybė atvaizduoti trūkstamus programinės įrangos atnaujinimus ir pataisas valdymo konsolėje, su CVE identifikacine informacija ir nuoroda į CVE (angl. common vulnerability and exposure) duomenų bazę.
109.	Kritinių ir svarbių pataisų atnaujinimas turi būti vykdomas automatiškai. Turi būti galima nustatyti atnaujinimo vykdymo grafiką.
110.	Turi būti galimybė daryti išimtis pagal politiką tam tikros versijos programinės įrangos atnaujinimams, įskaitant paslaugų paketus (angl. service pack).
111.	Galimybė patikrinti kokia programinė įranga yra įdiegta darbo vietose ir identifikuoti trūkstamus atnaujinimus.
112.	Minimaliai turi būti galimybė valdyti šios programinės įrangos atnaujinimus: .NET Framework, Acrobat Reader, Adobe Acrobat, Adobe Flash, Apple Quicktime, Ccleaner, Citrix, Excel, Firefox, Google chrome, Internet explorer, Opera, Safari, Skype, Thunderbird, Vmware, Winzip, MS Team, Onedrive.
Centralizuotos administravimo konsolės diegimo reikalavimai:	
113.	Windows Server 2008 R2; Windows Server 2012; Windows Server 2012 R2.
114.	Red Hat Enterprise Linux 6/7 32 ir 64-bit, SUSE Linux Enterprise Server 11 32 ir 64-bit, SUSE Linux Enterprise Desktop 11 32 ir 64-bit, openSUSE Linux 15, Debian GNU Linux 9, 10 32 ir 64-bit; Ubuntu Ubuntu 16, 18, 20.
Atitikimas vertinimams iš nepriklausomų AV testavimo laboratorijų:	

115.	av-comparatives best protection įvertinimas 2019/2020 metais
Bendri reikalavimai tiekėjui:	
116.	Turi būti užtikrintas 3 metų gamintojo palaikymas telefonu/el. paštu anglų kalba 24 val. per parą 7 dienas per savaitę.
117.	Turi būti užtikrintas 3 metų Tiekėjo palaikymas lietuvių kalba telefonu/el. paštu darbo valandomis (8.00 - 17.00) darbo dienomis.
118.	Antivirus/Antispam sistema turi gauti programinės įrangos gamintojo išleidžiamus atnaujinimus, pagerinimus į naujas versijas ir palaikymą trejų metų laikotarpyje.
119.	Tiekėjas turi atlikti diegimo ir jei reikalinga migravimo nuo šiuo metu UŽSAKOVO naudojamo F-Secure antivirus sprendimo darbus, **šių darbų kaina turi būti įtraukta į programinės įrangos kainą**. Tiekėjas turės pilnai įdiegti siūlomą programinę įrangą apimant tiek centrinę sistemos dalį tiek kompiuterizuotas darbo vietas. Pirkimo pasiūlyme turi būti pateiktas detalus migravimo darbų aprašymas, pateiktas migravimo darbų planas nurodant darbų trukmes. Visi diegimo darbai turi būti atlikti per 10 darbo dienų nuo sutarties pasirašymo dienos.
120.	Tiekėjas turi apmokyti ne mažiau kaip 2 UŽSAKOVO darbuotojus siūlomos programinės įrangos gamintojo mokymo centre. Tiekėjas turi suteikti mokymus diegimo, konfigūravimo, valdymo ir problemų sprendimo temomis, kurie suteiktų galimybę UŽSAKOVUI pilnai administruoti perkamą programinę įrangą savo infrastruktūroje. Mokymai turi būti suteikti jei siūlomas sprendimas skiriasi nuo UŽSAKOVO šiuo metu naudojamo F-Secure sprendimo. Į pasiūlymo kainą turi būti įtrauktos visos susijusios išlaidos, t.y. mokymo kursų kaina, kelionės ir pragyvenimo išlaidos jei mokymai bus vykdomi ne Lietuvos Respublikos teritorijoje.

_____

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Valstybinė mokesčių inspekcija prie Lietuvos Respublikos finansų ministerijos 188659752, Vasario 16-osios g. 14, Vilniaus m., Vilniaus m. sav. UAB "NBCS" 301817848, Jono Kazlausko g. 21, Vilniaus m., Vilniaus m. sav.
Dokumento pavadinimas (antraštė)	ANTIVIRUSINĖS PROGRAMINĖS ĮRANGOS VIEŠOJO PIRKIMO SUTARTIS
Dokumento registracijos data ir numeris	2021-03-08 Nr. (1.10-04-2 E) 22-27
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	Edita Janušienė, VMI prie FM viršininkas, Vadovybė
Sertifikatas išduotas	EDITA JANUŠIENĖ, Valstybinė mokesčių inspekcija prie FM LT
Parašo sukūrimo data ir laikas	2021-03-08 12:35:27 (GMT+02:00)
Parašo formatas	XAdES-T
Laiko žymoje nurodytas laikas	2021-03-08 12:35:32 (GMT+02:00)
Informacija apie sertifikavimo paslaugų teikėją	ADIC CA-B, Asmens dokumentu israsymo centras prie LR VRM LT
Sertifikato galiojimo laikas	2018-09-25 10:38:27 – 2021-09-24 10:38:27
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	ARTIOM,MASLOV, atstovas, UAB "NBCS"
Sertifikatas išduotas	ARTIOM,MASLOV LT
Parašo sukūrimo data ir laikas	2021-03-08 13:41:04 (GMT+02:00)
Parašo formatas	XAdES-T
Laiko žymoje nurodytas laikas	2021-03-08 13:41:46 (GMT+02:00)
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016, AS Sertifitseerimiskeskus EE
Sertifikato galiojimo laikas	2019-10-01 14:09:11 – 2024-09-29 23:59:59
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	"Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "RCSC IssuingCA, VI Registru centras - i.k. 124110246 LT" išduotą sertifikatą "Darbo organizavimo ir dokumentų valdymo sistema (DODVS), VMI prie LR finansų ministerijos, į.k.188659752 LT", sertifikatas galioja nuo 2018-12-21 14:05:28 iki 2021-12-20 14:05:28
Pagrindinio dokumento priedų skaičius	–
Pagrindinio dokumento pridedamų dokumentų skaičius	–
Pridedamo dokumento sudarytojas (-ai)	–
Pridedamo dokumento pavadinimas (antraštė)	–
Pridedamo dokumento registracijos data ir numeris	–
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Dokumentų valdymo sistema Avilys, versija 3.5.38
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja (2021-03-08 13:48:45)
Paieškos nuoroda	–
Papildomi metaduomenys	Nuorašą suformavo 2021-03-08 13:48:45 Dokumentų valdymo sistema Avilys