PASIŪLYMAS KONKURSUI
ANTIVIRUSINĖS PROGRAMINĖS ĮRANGOS VIEŠASIS PIRKIMAS

2021-02-25
(Data)
Vilnius
(Vieta)

TIEKĖJO pavadinimas /*Jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių pavadinimai*/	UAB „NBCS“
TIEKĖJO kodas /*Jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių pavadinimai*/	301817848
TIEKĖJO adresas /*Jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių adresai*/	J.Kazlausko g. 21 LT-08314 Vilnius
Telefono numeris	+370 5 2764563
El. pašto adresas	info@nbcs.lt
Bankas	AB „SEB“ Bankas
Sąskaitos numeris	LT41 7044 0600 0831 9438

Pastaba. Pildoma, jei TIEKĖJAS ketina pasitelkti, subtiekėją (-us) ar specialistus ir ekspertus, kuriais bus remiamasi įrodinėjant TIEKĖJO kvalifikaciją ir vykdant pirkimo sutartį, tačiau pasiūlymo pateikimo metu jie nėra TIEKĖJO ar jo pasitelkiamo (ų) subtiekėjo(ų) darbuotojai, tačiau laimėjimo atveju bus įdarbinti

Subtiekėjo (-ų) pavadinimas (-ai)	
Subtiekėjo (-ų) kodas (-ai)	
Subtiekėjo (-ų) adresas (-ai)	
Specialistai ir ekspertai, kuriais bus remiamasi įrodinėjant TIEKĖJO kvalifikaciją ir vykdant pirkimo sutartį, tačiau jie nėra TIEKĖJO ar TIEKĖJO pasitelkiamo (ų) subtiekėjo (-ų) darbuotojai pasiūlymo pateikimo metu, bet laimėjimo atveju būtų įdarbinti	
Įsipareigojimų dalis (nurodant konkrečius pagal pirkimo sutartį prisiimamus įsipareigojimus), kuriai ketinama pasitelkti subtiekėją (-us),	

Bus remiamasi šių ūkio subjektų pajėgumais:

Eil. Nr.	Nurodomas ūkio subjekto pavadinimas ir kokiems reikalavimams pagrįsti remiamasi jų pajėgumais

Pastaba. Pildoma tuomet, jei bus remiamasi kitų ūkio subjektų pajėgumais

Šiuo PASIŪLYMU KONKURSUI pažymime, kad sutinkame su visomis KONKURSO sąlygomis, nustatytomis KONKURSO DOKUMENTUOSE.

Pareiškiame, kad esame suinteresuoti dalyvauti KONKURSE ir sudaryti pirkimo sutartį pagal KONKURSO DOKUMENTUOSE nustatytus reikalavimus.

Pareiškiame, kad pasiūlymas yra parengtas nepasinaudojant ryšiais, informacija, sulygintais duomenimis arba susitarimu su kitais ūkio subjektais arba asmenimis.

Pranešame, kad rūpestingai išnagrinėję KONKURSO DOKUMENTUS, esame pasirengę atlikti PREKIŲ TIEKIMĄ pagal KONKURSO DOKUMENTŲ reikalavimus už:

	Kaina skaičiais	Kaina žodžiais
PREKIŲ TIEKIMO kaina EUR be PVM	106.500,00	Šimtas šeši tūkstančiai penki šimtai eurų
PREKIŲ TIEKIMO kaina EUR su PVM	128.865,00	Šimtas dvidešimt aštuoni tūkstančiai aštuoni šimtai šešiasdešimt penki eurai

Detalizuojame PREKIŲ TIEKIMO kainą:

Eil. Nr.	Pavadinimas	Gamintojo PREKĖS pavadinimas, PREKĖS kodas	Kiekis, vnt. (a)	Vieneto kaina, Eur be PVM (b)	Vieneto kaina, Eur su PVM (c)	Suma, Eur su PVM (d=a*c)
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	106.500,00	128.865,00	128.865,00
2.	UŽSAKOVO darbuotojo apmokymas eksploatuoti ir administruoti siūlomą programinę įrangą gamintojo mokymo centre.	-	2	0,00	0,00	0,00
3.				PREKIŲ TIEKIMO kaina Eur su PVM:		128.865,00

Siūlomų PREKIŲ atitikimas techniniams reikalavimams:

Eil. nr.	Reikalavimai	Tiekėjo siūloma parametro reikšmė
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.	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.	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.	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).	Sistema naudoja užklausomis paremtą žalingų programų aprašų reputacijos tikrinimą (panaudojant debesų kompiuterijos technologiją).
5.	Sprendimas turėtų naudoti hešuotą talpą žalingų programų laikymui.	Sprendimas naudoja 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.	Sprendimas darbo vietoms ir tarnybinėms stotims turi ne mažiau dviejų skenavimo variklių virusų ir šnipinėjimo programų aptikimui ir 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).	Sprendimas gali 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).	Žalingų programų signatūrų ir skenavimo variklio atnaujinimas kompiuterinėse darbo vietose gali vykti tarp kompiuterinių darbo vietų esančių tame pačiame lokaliame kompiuteriniame tinkle, tam, kad nebūtų apkraunamas interneto ryšys. Tokio atnaujinimo tipui nereikia diegti tarpinės atnaujinimų tarnybinės stoties ar vietinės atnaujinimų tarnybinės stoties. Taip pat sistema geba 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.	Sprendimas užtikrina 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.	Yra 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.	Skenuoja POP3, SMTP ir IMAP4 srautą realiu laiku nuo žalingų programų.
12.	Turi skenuoti HTTP srautą nuo virusų prieš duomenų perdavimą į internetinę naršyklę.	Skenuoja HTTP srautą nuo virusų prieš duomenų perdavimą į internetinę naršyklę.
13.	Palaikomos kalbos: anglų, prancūzų, vokiečių, lenkų, rusų.	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.	Automatinis atnaujinimas su atsarginiais atnaujinimo kanalais t.y. šalia pagrindinio atnaujinimo kanalo yra papildomai nemažiau kaip du alternatyvūs atnaujinimų pateikimo kanalai.

15.	Automatinis žalingų programų šalinimas, turi būti konfigūruojama administratoriaus (leisti/neleisti).	Automatinis žalingų programų šalinimas, konfigūruojama administratoriaus (leisti/neleisti).
16.	Rankinis ir pagal nustatytą planą sistemos skenavimas, turi būti konfigūruojamas administratoriaus arba pačio vartotojo jei administratorius tokią galimybę suteikė.	Rankinis ir pagal nustatytą planą sistemos skenavimas, 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.	Virusų ir šnipinėjimo (angl. Spyware) skenavimo istorija atvaizduojama tiek kompiuterinėje darbo vietoje, tiek valdymo konsolėje, taip pat turi yra galimybė panaikinti statistiką.
18.	Turi būti renkama statistika apie skenuotus failus, leidžiamas programas, išvalytus failus ir blokuotas programas.	Renkama statistika apie skenuotus failus, leidžiamas programas, išvalytus failus ir blokuotas programas.
19.	Skenavimo variklis turi veikti aprašu ir euristika paremtomis technologijomis.	Skenavimo variklis veikia aprašu ir euristika paremtomis technologijomis.
20.	„Rootkit“ žalingos programos aptikimas ir šalinimas.	„Rootkit“ žalingos programos aptikimas ir šalinimas.
21.	Žalingų programų aptikimas remiantis jų elgsena.	Žalingų programų aptikimas remiantis jų elgsena.
22.	Turi būti integruota interneto naršymo apsaugos funkcija, kuri turi identifikuoti žalingus internetinius puslapius ir juos blokuoti.	Integruota interneto naršymo apsaugos funkcija, kuri identifikuoja žalingus internetinius puslapius ir juos blokuoja.
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.	Sprendimas turi 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.	Naršymo apsauga saugo internetinę naršyklę ir jos įskiepius nuo žinomų pažeidžiamumų.
25.	Internetinio turinio kontrolė turi leisti blokuoti svetaines su nepriimtinu turiniu.	Internetinio turinio kontrolė leidžia blokuoti svetaines su nepriimtinu turiniu.
26.	Turi būti atliekamas visų aktyvių procesų atminties intervalų skenavimas.	Atliekamas visų aktyvių procesų atminties intervalų skenavimas.
27.	Turi būti integruota asmeninė ugniasienės, apsaugos nuo įsiveržimo sistema technologija kompiuterinėms darbo vietoms.	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.	Ugniasienės taisyklės ir profiliai 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.	Galimybė kontroliuoti prieigą prie tinklo remiantis aplikacija.
30.	Galimybė registruoti įvykius ir įspėti apie juos atsiradus kai pažeidžiama apsaugos nuo įsiveržimo sistemos taisyklė.	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.	Galimybė administratoriui blokuoti DNS užklausas iš „hosto“ domenams su žalinga reputacija.

32.	Centralizuota aplikacijų kontrolė ir prisijungimo į internetą šiomis aplikacijomis blokavimo galimybės.	Centralizuota aplikacijų kontrolė ir prisijungimo į internetą šiomis aplikacijomis blokavimo galimybės.
33.	Turi būti integruota išorinių įrenginių kontrolės funkcionalumas.	Integruota išorinių įrenginių kontrolės funkcionalumas.
34.	Turi būti galimybė automatiškai šalinti konfliktuojančią programinę įrangą saugumo programinės įrangos diegimo metu.	Galimybė automatiškai šalinti konfliktuojančią programinę įrangą saugumo programinės įrangos diegimo metu.
35.	Turi būti galimybė iš vienos centrinės konsolės atlikti sistemos nustatymus.	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).	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 (pateikta versija galinti palaikyti šią OS); Windows XP 32-bit SP3 (esant poreikiui bus pateikta versija diegimui šioje OS); Windows XP Home Edition SP2/SP3 (esant poreikiui bus pateikta versija diegimui šioje OS); Windows XP Professional Edition SP2/SP3 (esant poreikiui bus 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-	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.	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.	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.	Saugo įeinantį, išeinantį ir vidinį el. pašto srautą, bei MS Exchange viešus katalogus nuo kenkėjiškų programų, bei atlieka turinio ir priedėlių skenavimą.
40.	Skenavimo variklis turi būti atnaujinamas automatiškai.	Skenavimo variklis 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.	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.	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.	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.	Slaptažodžiu apsaugotus archyvus galima laikyti ir taikyti saugumo politiką, kaip nesaugiems.
45.	Įtartini ir nesaugūs priedėliai gali būti pašalinti iš el. pašto.	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.	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.	Virusai yra 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.	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.	Technologija yra 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.	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	Efektyviai kovai su nepageidaujamu paštu 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 aptinkamas įvairiose kalbose, įskaitant sunkiai

	sunkiai analizuojamus kelių baitų simbolius, tokių kalbų, kaip kinų ar japonų.	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.	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	Sistema stebi 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.	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.	Sistema gali integruotis su trečių šalių tarpinėmis tarnybinėmis stotimis per ICAP protokolą.
56.	Turinio filtravimo galimybės, kurios turi būti nustatomos pagal failų tipą, dydį, pavadinimą.	Turinio filtravimo galimybės, kurios nustatomos pagal failų tipą, dydį, pavadinimą.
57.	ActiveX ir Java koduotės skenavimo/blokavimo galimybės.	ActiveX ir Java koduotės skenavimo/blokavimo galimybės.
58.	Turi būti galimybė įspėjimo tekstus (pav. rinkmena užkrėsta virusu) keisti ir naudoti UTF-8 koduotės simbolius.	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.	Sistema aptinka virusus orientuotus į Windows, DOS, Microsoft Office, VBS, Linux ir kitas aplinkas.
60.	Virusų aprašų bazė turi būti atnaujinama automatiškai.	Virusų aprašų bazė atnaujinama automatiškai.
61.	Skenavimo variklis turi palaikyti ir skenuoti įvarius archyvavimo formatus (ZIP, ARJ, LZH, CAB, RAR, TAR, GZIP, BZIP2).	Skenavimo variklis palaiko ir skenuoja 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.	Galimybė aptikti nepageidaujamą el. paštą (brukalą) prieigos vartuose (prieš jiems patenkant į el. pašto serverį) tiek SMTP tiek POP srautams, todėl sistema turi 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.	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.	Valdymo konsolė turi 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.	Antivirusinė programinė įranga kompiuteriams (stacionarams ir nešiojamiems) ir tarnybinėms stotims, antivirusinė programinė įranga Microsoft Exchange pašto tarnybiniai stočiai ir antivirusinė prieigos vartų programinė įranga valdoma iš vienos centralizuoto valdymo konsolės.
66.	Konsolė turi pateikti automatiškai ataskaitas apie naudojamas aplikacijas administratoriui.	Konsolė pateikia automatiškai ataskaitas apie naudojamas aplikacijas administratoriui.
67.	Ataskaitas turi būti galima peržiūrėti internetinėje naršyklėje ir taip pat turi būti galima eksportuoti į kitus formatus.	Ataskaitas galima peržiūrėti internetinėje naršyklėje ir taip pat galima eksportuoti į kitus formatus.
68.	Galimybė administratoriui blokuoti aplikacijas.	Galimybė administratoriui blokuoti aplikacijas.
69.	Galimybė konfigūruoti sistemų skenavimo tvarkaraštį.	Galimybė konfigūruoti sistemų skenavimo tvarkaraštį.
70.	Galimybė nuotolinių būdu valdyti karantiną.	Galimybė nuotolinių būdu valdyti karantiną.
71.	Galimybė įtraukti į baltą sąrašą (angl. Whitelisting) tinklalapius remiantis URL reputacijos analize.	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.	Žalingos programos atakos metu, sprendimas turi 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.	Atnaujinimas programinės įrangos aprašų duomenų bazių darbo vietoms/tarnybinėms stotims 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.	Ataskaitų servisas (paremtas web naršykle) suteikia 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.	Galimybė sukurti taisyklių "medį" detalesniems nustatymams.
76.	Galimybė peržiūrėti nustatymus/savybes domenui arba "hostui".	Galimybė peržiūrėti nustatymus/savybes domenui arba "hostui".
77.	Galimybė importuoti naujus "hostus" į specifinius domenus.	Galimybė importuoti naujus "hostus" į specifinius domenus.
78.	Automatinis „hostų“ suradimas iš Windows domeno.	Automatinis „hostų“ suradimas iš Windows domeno.
79.	„Hostų“ ar domenų perkėlimo galimybė naudojant "cut" ir "paste" operacijas.	„Hostų“ ar domenų perkėlimo galimybė naudojant "cut" ir "paste" operacijas.
80.	Valdymo konsolė turėtų turėti galimybę būti vieninteliu atnaujinimo tašku ir galėti	Valdymo konsolė turi galimybę būti vieninteliu atnaujinimo tašku ir gali

	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.	valdyti programinės įrangos pagerinimo procesus, taip pat nešiojamiems kompiuteriams užtikrinami kiti atsinaujinimo šaltiniai jei toks kompiuteris yra ne tinkle tam tikru laiko periodu.
81.	Nustatymų išplatinimas vartotojams ir galimybė paslėpti juos nuo vartotojo.	Nustatymų išplatinimas vartotojams ir galimybė paslėpti juos nuo vartotojo.
82.	Galimybė daryti išimtis pasirinktų plėtinių skenavimui (kad būtų neskenuojami).	Galimybė daryti išimtis pasirinktų plėtinių skenavimui (kad būtų neskenuojami).
83.	Galimybė daryti skenavimo išimtis remiantis pakaitos simboliais (angl. Wildcards).	Galimybė daryti skenavimo išimtis remiantis pakaitos simboliais (angl. Wildcards).
84.	Galimybė pasirinkti ar tinklo diskai turi būti įtraukti į realaus laiko skenavimą.	Galimybė pasirinkti ar tinklo diskai turi būti įtraukti į realaus laiko skenavimą.
85.	Galimybė pasirinkti ar sekimo slapukai (angl. Tracking cookies) turi būti skenuojami.	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.	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.	Galimybė nustatyti patikimus HTTP puslapius, kurie nebus skenuojami web srauto skenavimo metu.
88.	Įspėjimo žinučių siuntimas skirtingais el. pašto adresais priklausomai nuo įspėjimo tipo.	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.	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.	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.	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.	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.	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.	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.	Centrinis valdymas palaiko tiek MS Windows, tiek Linux platformas administruojamų ir saugumo įrenginių.
96.	Galimybė matyti paskutinės konfigūracijos laiko štampą.	Galimybė matyti paskutinės konfigūracijos laiko štampą.

97.	Galimybė rūšiuoti prisijungusius saugumo komponentus (angl. host) ir rodyti neprisijungusius.	Galimybė rūšiuoti prisijungusius saugumo komponentus (angl. host) ir rodyti neprisijungusius.
98.	Galimybė matyti saugumo komponento WINS savybes, IP, DNS ir operacines sistemos informaciją.	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.	Diegimas tinkle į saugumo komponentą remiantis IP adresu arba saugumo komponento pavadinimu.
100.	Galimybė sukurti MSI instaliacinį failą diegimo tikslams.	Galimybė sukurti MSI instaliacinį failą diegimo tikslams.
101.	Galimybė centralizuoto diegimo tikslais sukurti rinkmeną paremtą paruoštuko (angl. script) metodu.	Galimybė centralizuoto diegimo tikslais sukurti rinkmeną paremtą paruoštuko (angl. script) metodu.
102.	Galimybė blokuoti kompiuterių su sena virusų aprašų duomenų baze prieigą prie interneto.	Galimybė blokuoti kompiuterių su sena virusų aprašų duomenų baze prieigą prie interneto.
103.	Pavienių žalingų programų aprašų atnaujinimo galimybė.	Pavienių žalingų programų aprašų atnaujinimo galimybė.
104.	Vietinis atnaujinimo aprašų išdalinimas tinklo kompiuteriams su galimybe atnaujinti pavienius aprašus.	Vietinis atnaujinimo aprašų išdalinimas tinklo kompiuteriams su galimybe atnaujinti pavienius aprašus.
105.	Galimybė valdyti linux sistemų klientus iš centrinės valdymo konsolės.	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.	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.	Atnaujinimas 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.	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.	Kritinių ir svarbių pataisų atnaujinimas vykdomas automatiškai. 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).	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.	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.	Minimaliai yra 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.	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.	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	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.	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.	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.	Antivirus/Antispam sistema gaus 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.	Siūlome šiuo metu UŽSAKOVO naudojamo F-Secure antivirus sprendimą.
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	Siūlome šiuo metu UŽSAKOVO naudojamo F-Secure antivirus sprendimą.

	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.	

Kartu su PASIŪLYMU KONKURSUI pateikiami šie dokumentai:

Eil. Nr.	Pateiktų dokumentų pavadinimas	Dokumento puslapių skaičius
1.	V. Gricukės įgaliojimas_konfidencialu	1
2.	Jungtinė registrų centro pažyma	2
3.	UAB NBCS EBVPD	13
4.	Gamintojo patvirtinimo raštas_konfidencialu	1
5.	ISO 9001 sertifikatas	1

Ši pasiūlyme nurodyta informacija yra konfidenciali /*perkančioji organizacija šios informacijos negali atskleisti tretiesiems asmenims*/:

Eil. Nr.	Pateikto dokumento pavadinimas (rekomenduojama pavadinime vartoti žodį „Konfidencialu“)	Dokumento puslapių skaičius
1.	V. Gricukės įgaliojimas_konfidencialu	1
2.	Gamintojo patvirtinimo raštas_konfidencialu	1

CVP IS priemonėmis pateikdamas pasiūlymą, patvirtinu, kad dokumentų skaitmeninės kopijos ir elektroninėmis priemonėmis pateikti duomenys yra tikri.

Tuo atveju, jeigu mūsų KONKURSO pasiūlymas būtų priimtas, UŽSAKOVUI pareikalavus įsipareigojame kuo greičiau pasirašyti pirkimo sutartį atitinkančią KONKURSO DOKUMENTŲ reikalavimus, ir pradėti PREKIŲ TIEKIMĄ.

Mūsų pasiūlymas įsigalioja nuo KONKURSO pasiūlymų pateikimo termino pabaigos, ir galioja 3 mėnesius nuo KONKURSO pasiūlymų pateikimo termino pabaigos dienos.

Patvirtiname, kad nesudarėme jokių sutarčių, raštu ar žodžiu, su bet kokiomis trečiosiomis šalimis dėl PREKIŲ TIEKIMO rezultato ar bet kokio jo elemento perleidimo ateityje, taip pat, kad PREKIŲ TIEKIMO rezultato ar bet kokio jo elemento atžvilgiu nėra jokių neįvykdytų trečiųjų šalių teisių, įskaitant, bet neatsiribojant nuoma, panauda ir kt.

Patvirtiname, kad kol bus parengta ir sudaryta oficiali pirkimo sutartis, šis pasiūlymas su UŽSAKOVO raštu pateiktu pasiūlymo akceptavimu galioja kaip įpareigojanti sutartis.

Vilma Gricukė

(vardas, pavardė) (parašas)

Dokumentą elektroniniu parašu pasirašė VILMA,GRICUKĖ
Data: 2021-02-25 17:54:48