Konkurso sąlygų
2 priedas

UAB NRD CS
Gynėjų g. 14, LT-01109, Vilnius,
Telefonas +370 5 219 1919, el. paštas info@nrdcs.lt
duomenys kaupiami ir saugomi Juridinių asmenų registre
Įmonės kodas 303115085, PVM kodas LT100008214514

Nacionaliniam kibernetinio saugumo centrui
prie Krašto apsaugos ministerijos

PASIŪLYMAS
DĖL KENKSMINGO KODO ANALIZĖS PROGRAMINĖS ĮRANGOS LICENCIJOS

2020-10-05
(Data)
Vilnius
(Sudarymo vieta)

Tiekėjo pavadinimas, kodas, pridėtinės vertės mokesčio (toliau – PVM) mokėtojo kodas *(jeigu dalyvauja ūkio subjektų grupė, surašomi visų dalyvių duomenys)*	UAB NRD CS Juridinio asmens kodas 303115085 PVM mokėtojo kodas LT100008214514
Tiekėjo adresas *(jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių adresai)*	Gynėjų g. 14, LT-01109 Vilnius
Asmens, pasirašiusio pasiūlymą saugiu elektroniniu parašu vardas, pavardė, pareigos *(kai pasiūlymą elektroniniu parašu patvirtina ne įmonės vadovas, o įgaliotas asmuo, pasiūlyme pateikiama įgaliojimo ar kito dokumento, suteikiančio teisę pasirašyti tiekėjo pasiūlymą, skaitmeninė kopija)*	Komercijos direktorius Darius Dulskas
Telefono numeris, fakso numeris	+370 5 219 1919
El. pašto adresas	info@nrdcs.lt
Tiekėjo banko rekvizitai	A. s. Nr. LT627290099082023785 AS „Citadele banka“ Lietuvos filialas Banko kodas 72900

Pildoma, jei tiekėjas ketina pasitelkti subtiekėją (-us), ūkio subjektą (-us), kurių pajėgumais remiasi:

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) pirkimo dokumentuose ir skelbime apie pirkimą;
2) kituose pirkimo dokumentuose (jų paaiškinimuose, papildymuose);
2. Pasirašydami CVP IS priemonėmis pateiktą pasiūlymą saugiu elektroniniu parašu, patvirtiname, kad dokumentų skaitmeninės kopijos ir elektroninėmis priemonėmis pateikti duomenys yra tikri.

Mes siūlome šias Prekes:

1 lentelė.

Eil. Nr.	**Pirkimo objektas**	**Tiekėjo siūlomų prekių gamintojo suteiktas pavadinimas (tipas, modelis)** *(pildo tiekėjas)*	**Prekių kiekis (vnt.)**	**Vieneto įkainis, Eur be PVM***	**PVM EUR****	**Bendra kaina, Eur su PVM**
1	***2***	***3***	***4***	***5***	***6***	***7***
1.	Kenksmingo kodo analizės programinės įrangos licencija	**„Falcon Sandbox On Prem - Unlimited**	**1**	***82000,00***	***17,220***	***99,220***

Bendra pasiūlymo kaina yra <u>devyniasdešimt devyni tūkstančiai du šimtai dvidešimt</u> eurų <u>0</u> ct (*nurodoma kaina žodžiais***).**

Tais atvejais, kai pagal galiojančius teisės aktus tiekėjui nereikia mokėti PVM, jis nurodo priežastis, dėl kurių PVM nemokamas_____.

_____
** Pateikiamas įkainis, nurodant įrašoma 2 (du) skaičius po kablelio.*
*** Jei 6 stulpelis „PVM“ nepildomas, nurodomos priežastys, dėl kurių PVM nemokamas.*

Tiekėjas patvirtina, kad kainos nurodytos su PVM, muito, prekių transportavimo iki Gavėjo sandėlio ir kitomis išlaidomis, galinčiomis turėti įtakos tiekiamų prekių kainai.
Tiekėjas patvirtina, kad prekės bus pristatytos prekių viešojo pirkimo–pardavimo sutartyje numatytomis pagrindinėmis sąlygomis ir adresais.
Tiekėjas patvirtina, kad yra susipažinęs ir sutinka su Pirkėjo pateiktomis sutarties sąlygomis *(konkurso sąlygų 7 priedas*) bei užtikrina, kad pasiūlymo 2 lentelėje nurodytos prekės atitiks techninėje specifikacijoje *(konkurso sąlygų 1 priedas)* nustatytus reikalavimus**.**

Siūlomos prekės visiškai atitinka pirkimo dokumentuose nurodytus techninius reikalavimus ir jų savybės tokios:

2 lentelė. Siūlomos prekės techniniai rodikliai:

Eil. Nr.	Prekėms keliami reikalavimai	Tiekėjų siūlomų prekių detalus aprašymas* *(pildo tiekėjas)*
1.	**Bendrieji reikalavimai:**	
1.1.	Kenksmingo kodo analizės programinės įrangos (toliau – PĮ) licencija (toliau – licencija) turi būti išduota gamintojo ar jo įgalioto asmens.	Kenksmingo kodo analizės programinės įrangos (toliau – PĮ) licencija (toliau – licencija) bus išduota gamintojo.
1.2.	Licencijos duomenys siunčiami tiesiogiai Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos (toliau -NKSC) adresu licencijos@cert.lt	Licencijos duomenys siunčiami tiesiogiai Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos (toliau -NKSC) adresu licencijos@cert.lt
1.3.	Tiekėjas turi pateikti nuorodą ar nuorodas į gamintojo interneto puslapį, kuriame yra tiksli pasiūlymą atitinkančios licencijos techninė specifikacija arba pateikti gamintojo patvirtintą siūlomos licencijos aprašymą.	Pateikiame nuorodas: https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/ https://www.crowdstrike.com/wp-content/uploads/2020/03/FalconXSandboxDatasheet.pdf
1.4.	Tiekėjas turi užtikrinti, kad gamintojas nėra paskelbęs žinios apie PĮ gamybos arba tobulinimo nutraukimą (pvz., angl. *end of life time* arba *Discontinued*).	Tiekėjas užtikrina, kad gamintojas nėra paskelbęs žinios apie PĮ gamybos arba tobulinimo nutraukimą (pvz., angl. *end of life time* arba *Discontinued*).
2.	**Prekių techninės charakteristikos:**	
2.1.	Licencija turi atitikti žemiau pateiktus reikalavimus (perkančiosios organizacijos testuota **„Falcon Sandbox”** PĮ licencija atitinka žemiau pateiktus reikalavimus, todėl siūlydamas šią įrangą tiekėjas papildomai neįpareigojamas pateikti įrodymų dėl jos atitikties žemiau nustatytiems reikalavimams).	Licencija atitinka žemiau pateiktus reikalavimus. Tiekėjas siūlo perkančiosios organizacijos testuotą ,,Falcon Sandbox, On Prem - Unlimited“ PĮ licenciją, kuri atitinka žemiau pateiktus reikalavimus, todėl, siūlydamas šią įrangą, tiekėjas papildomai neteiks įrodymų dėl jos atitikties žemiau nustatytiems reikalavimams.
2.2.	Licencija privalo neriboti analizuojamų failų kiekio per dieną/mėn. PĮ analizių kiekis per dieną gali būti priklausomas tik nuo paskirtos techninės įrangos pajėgumo.	Licencija neriboja analizuojamų failų kiekio per dieną/mėn. PĮ analizių kiekis per dieną gali būti priklausomas tik nuo paskirtos techninės įrangos pajėgumo.
2.3.	PĮ privalo turėti grafinę valdymo sąsaja per interneto naršyklę (angl. Web GUI), kuri nereikalauja jokios papildomos programos įdiegimo ir turėti šį funkcionalumą: - galimybę kurti ir valdyti nepriklausomas aplinkas (angl. client) pagal pasiekiamumą bei funkcionalumą;	PĮ turi grafinę valdymo sąsaja per interneto naršyklę (angl. Web GUI), kuri nereikalauja jokios papildomos programos įdiegimo ir turi šį funkcionalumą: - galimybę kurti ir valdyti nepriklausomas aplinkas (angl. client) pagal pasiekiamumą bei funkcionalumą;

	- galimybę kurti naudotojus su skirtingo lygio teisėmis; - kenkėjiško kodo analizavimo statistikos pateikimą; - techninės įrangos apkrovos stebėseną; - galimybę valdyti integruojamus papildinius ir indikatorių (IOC) šaltinius. - turėti galimybę veikti infrastruktūroje neturinčioje interneto ryšio.	- galimybę kurti naudotojus su skirtingo lygio teisėmis; - kenkėjiško kodo analizavimo statistikos pateikimą; - techninės įrangos apkrovos stebėseną; - galimybę valdyti integruojamus papildinius ir indikatorių (IOC) šaltinius. - turėti galimybę veikti infrastruktūroje neturinčioje interneto ryšio.
2.4.	Sistemos būsenos pokyčių įvertinimas prieš ir po kodo paleidimą, nėra priimtinas. PĮ turi gebėti aptikti: - kenkėjišką kodą; - polimorfinį kodą; - APT; - išnaudojimo kodą (angl. exploits, web exploits); - branduolio lygmens kenksmingą kodą (angl. Rootkits); PĮ turi gebėti atpažinti kenkėjiško kodo kampanijas pagal joms būdingus indikatorius ir elgseną. PĮ turi gebėti analizuoti objektus šiose aplinkose: Windows XP/Vista/7/8/10 (x64 ir x86) ir Linux Ubuntu/RHEL (x64 ir x86). PĮ privalo palaikyti, leisti pridėti naujų, modifikuoti esamas YARA paremtas taisykles. PĮ privalo leisti išplėsti detektavimo galimybes savo apsirašytomis taisyklėmis bei indikatoriais. PĮ turi sugebėti automatizuotai imituoti vartotojo veiksmus, tokius kaip pelės paspaudimas. PĮ turi gebėti pati paleisti įtartinus failus ir žiniatinklio (angl. web) objektus, ištestuoti juos skirtingose OS versijose su skirtingomis naršyklėmis, įskiepiais, aplikacijomis ir atlikti jų dinaminę analizę. PĮ turi gebėti detektuoti daugiapakopes (angl. multi-stage) atakas. PĮ turi gebėti analizuoti kenkėjiško kodo analizės metu parsiųstas ar sukurtas bylas, sukuriamą tinklo srautą (angl. network traffic). PĮ turi gebėti automatiškai analizuoti elektroniniu paštu gautus prisegtukus ar URL nuorodas.	Sistemos būsenos pokyčių įvertinimas prieš ir po kodo paleidimą, nėra priimtinas. PĮ geba aptikti: - kenkėjišką kodą; - polimorfinį kodą; - APT; - išnaudojimo kodą (angl. exploits, web exploits); - branduolio lygmens kenksmingą kodą (angl. Rootkits); PĮ turi gebėti atpažinti kenkėjiško kodo kampanijas pagal joms būdingus indikatorius ir elgseną. PĮ geba analizuoti objektus šiose aplinkose: Windows XP/Vista/7/8/10 (x64 ir x86) ir Linux Ubuntu/RHEL (x64 ir x86). PĮ palaiko, leidžia pridėti naujų, modifikuoti esamas YARA paremtas taisykles. PĮ leidžia išplėsti detektavimo galimybes savo apsirašytomis taisyklėmis bei indikatoriais. PĮ sugeba automatizuotai imituoti vartotojo veiksmus, tokius kaip pelės paspaudimas. PĮ geba pati paleisti įtartinus failus ir žiniatinklio (angl. web) objektus, ištestuoti juos skirtingose OS versijose su skirtingomis naršyklėmis, įskiepiais, aplikacijomis ir atlikti jų dinaminę analizę. PĮ geba detektuoti daugiapakopes (angl. multi-stage) atakas. PĮ geba analizuoti kenkėjiško kodo analizės metu parsiųstas ar sukurtas bylas, sukuriamą tinklo srautą (angl. network traffic).

	PĮ turi turėti HTTP protokolu paremtą programinio lygio sąsają (angl. API). PĮ turi palaikyti IDS sistemų naudojamas taisykles, analizės metu sugeneruojamo tinklo srauto patikrai vykdyti. PĮ turi galėti naudotis interneto ryšiu, siekiant tiksliau identifikuoti kenksmingą kodą. PĮ turi galėti maskuoti savo tikrąjį IP adresą analizės metu. PĮ turi galėti analizuoti objektus branduolio lygmens režime (angl. kernel mode). PĮ turi sugebėti perkrauti (angl. reboot) analizės aplinką kenkėjiško programinio kodo analizės metu. Jokia informacija negali būti siunčiama trečioms šalims ar į „debesį“, analizei, detektavimui ar informacijos dalinimuisi. PĮ privalo maskuoti virtualias analizės aplinkas taip, kad kenkėjiškas programinis kodas nesuprastų, kad yra leidžiamas virtualioje aplinkoje. PĮ turi gebėti analizuoti bylas ir URL nuorodas pagal kliento pareikalavimą, siekiant nustatyti ar jos yra kenksmingos. PĮ turi gebėti analizuoti kenkėjiško kodo analizės metu sukuriamus procesus (angl. services) ir operatyviosios atminties įrašus. PĮ turi gebėti leisti nustatyti atliekamos analizės prioritetą. PĮ turi gebėti leisti nustatyti atliekamos analizės vykdymo trukmę. PĮ turi turėti galimybę identifikuoti laikino neveiksnumo funkciją (angl. sleep) kenksmingame kode ir turi sugebėti vykdyti laiko paspartinimą, kad kenksmingas kodas tęstų tolimesnį jame numatytų instrukcijų/funkcijų vykdymą. PĮ turi gebėti validuoti visą pateikto analizei failo skaitmeninių certifikatų grandinę. PĮ turi gebėti vesti sisteminius įrašus apie kodo vykdymo iššaukimą (kaip VBA, JScript).	PĮ geba automatiškai analizuoti elektroniniu paštu gautus prisegtukus ar URL nuorodas. PĮ turi HTTP protokolu paremtą programinio lygio sąsają (angl. API). PĮ palaiko IDS sistemų naudojamas taisykles, analizės metu sugeneruojamo tinklo srauto patikrai vykdyti. PĮ gali naudotis interneto ryšiu, siekiant tiksliau identifikuoti kenksmingą kodą. PĮ gali maskuoti savo tikrąjį IP adresą analizės metu. PĮ gali analizuoti objektus branduolio lygmens režime (angl. kernel mode). PĮ sugeba perkrauti (angl. reboot) analizės aplinką kenkėjiško programinio kodo analizės metu. Jokia informacija negali būti siunčiama trečioms šalims ar į „debesį“, analizei, detektavimui ar informacijos dalinimuisi. PĮ maskuoja virtualias analizės aplinkas taip, kad kenkėjiškas programinis kodas nesuprastų, kad yra leidžiamas virtualioje aplinkoje. PĮ geba analizuoti bylas ir URL nuorodas pagal kliento pareikalavimą, siekiant nustatyti ar jos yra kenksmingos. PĮ geba analizuoti kenkėjiško kodo analizės metu sukuriamus procesus (angl. services) ir operatyviosios atminties įrašus. PĮ geba leisti nustatyti atliekamos analizės prioritetą. PĮ geba leisti nustatyti atliekamos analizės vykdymo trukmę. PĮ turi galimybę identifikuoti laikino neveiksnumo funkciją (angl. sleep) kenksmingame kode ir turi sugebėti vykdyti laiko paspartinimą, kad kenksmingas kodas tęstų tolimesnį jame numatytų instrukcijų/funkcijų vykdymą. PĮ geba validuoti visą pateikto analizei failo skaitmeninių certifikatų grandinę. PĮ geba vesti sisteminius įrašus apie kodo vykdymo iššaukimą (kaip VBA, JScript).

2.5.	Kenkėjiško kodo analizės įrenginys turi turėti galimybę automatiškai analizuoti objektus pagal pateiktą sąrašą. Sąrašas PĮ turi būti pateikiamas kokiu nors struktūrizuotu formatu, bet ne suvedinėjamas ranka po vieną įrašą.	Kenkėjiško kodo analizės įrenginys turi galimybę automatiškai analizuoti objektus pagal pateiktą sąrašą. Sąrašas PĮ bus pateikiamas kokiu nors struktūrizuotu formatu, bet ne suvedinėjamas ranka po vieną įrašą.
2.6.	PĮ turi gebėti atlikti tinklalapių statinę (tinklalapyje esančių nuorodų, „Javascript“ programinio kodo ir t.t.) ir dinaminę (imituojant vartotojo naršymą tinklalapyje sugeneruojamo srauto, parsiunčiamų failų) analizę.	PĮ geba atlikti tinklalapių statinę (tinklalapyje esančių nuorodų, „Javascript“ programinio kodo ir t.t.) ir dinaminę (imituojant vartotojo naršymą tinklalapyje sugeneruojamo srauto, parsiunčiamų failų) analizę.
2.7.	PĮ turi gebėti atlikti „Android“ operacinėms sistemoms skirtų failų (programų) analizę. PĮ turi gebėti analizuoti slaptažodžiu apsaugotus archyvus ir bylas: ace, arj, 7z, bzip2, gzip2, iso, rar, rev, tar, wim, xz, zip. PĮ turi gebėti atpažinti ir analizuoti analizei pateiktuose dokumentuose (MS Office, .pdf failuose) esančias makrokomandas, VBA/Javascript programinį kodą, URL nuorodas bei paslėptus failus. PĮ turi gebėti analizuoti bent šiuos populiarius bylų tipus pagal plėtinį: 7z, ace, apk, bat, bzip2, cab, chm, com, cpl, dll, doc, docx, eml, elf, exe, gzip2, hta, iso, jar, js, lnk, msg, pdf, pl, pv, pif, ppt, pptx, ppsx, ps1, psd1, psm1, pub, rar, rtf, src, sct, svg, swf, tar, vbe, vbs, xls, xlsx, xz, wim, wsf, zip. PĮ turi gebėti automatiškai atlikti pakartotinę analizę, jeigu pirminė buvo nesėkminga. Pakartotinės analizės bandymų kiekis – ne mažiau kaip 2. Turi gebėti atlikti tarpusavyje susijusių (angl. dependencies files) bylų analizę. PĮ turi gebėti atlikti statistinę bet kokio failo analizę. PĮ turi turėti išplėstinės paieškos pagal įvairius kriterijus galimybę. PĮ turi gebėti generuoti atliktą analizę apibendrinančias ataskaitas bent šiais formatais: html, json, pdf, xml PĮ turi gebėti vesti darbo sisteminius įrašus ir saugoti analizės metu sukuriamą tinklo srautą .pcap formatu. PĮ turi gebėti pateikti objekto analizę apibendrinančias išvadas.	PĮ geba atlikti „Android“ operacinėms sistemoms skirtų failų (programų) analizę. PĮ geba analizuoti slaptažodžiu apsaugotus archyvus ir bylas: ace, arj, 7z, bzip2, gzip2, iso, rar, rev, tar, wim, xz, zip. PĮ turi gebėti atpažinti ir analizuoti analizei pateiktuose dokumentuose (MS Office, .pdf failuose) esančias makrokomandas, VBA/Javascript programinį kodą, URL nuorodas bei paslėptus failus. PĮ geba analizuoti bent šiuos populiarius bylų tipus pagal plėtinį: 7z, ace, apk, bat, bzip2, cab, chm, com, cpl, dll, doc, docx, eml, elf, exe, gzip2, hta, iso, jar, js, lnk, msg, pdf, pl, pv, pif, ppt, pptx, ppsx, ps1, psd1, psm1, pub, rar, rtf, src, sct, svg, swf, tar, vbe, vbs, xls, xlsx, xz, wim, wsf, zip. PĮ geba automatiškai atlikti pakartotinę analizę, jeigu pirminė buvo nesėkminga. Pakartotinės analizės bandymų kiekis – ne mažiau kaip 2. Geba atlikti tarpusavyje susijusių (angl. dependencies files) bylų analizę. PĮ geba atlikti statistinę bet kokio failo analizę. PĮ turi išplėstinės paieškos pagal įvairius kriterijus galimybę. PĮ geba generuoti atliktą analizę apibendrinančias ataskaitas bent šiais formatais: html, json, pdf, xml PĮ geba vesti darbo sisteminius įrašus ir saugoti analizės metu sukuriamą tinklo srautą .pcap formatu. PĮ geba pateikti objekto analizę apibendrinančias išvadas.

	PĮ turi fiksuoti ir atvaizduoti dinaminės analizės metu veikiančių virtualių mašinų ekrano kopijas kas sekundę. PĮ turi galėti rūšiuoti analizės įvykius chronologiška seka. PĮ privalo turėti galimybę siųsti pranešimus apie identifikuotus įvykius bent šiais protokolais: - syslog (syslog, rsyslog, syslog-ng); - SMTP (informuoti el. paštu). PĮ privalo turėti galimybę siųsti pranešimus, aukščiau įvardintais protokolais, apie įvykius naudojant bent šiuos formatus: - tekstinį (angl. text); - JSON; - XML; PĮ privalo gebėti sugeneruotas ataskaitas patalpinti į struktūrizuotą rezultatų aplankalą, kuriame ataskaitos yra patalpinamos atskirais formatais: html/json/xml/ maec/openIOC PĮ privalo turėti galimybę siųsti pranešimus apie atliktą analizę el. paštu.	PĮ fiksuoja ir atvaizduoja dinaminės analizės metu veikiančių virtualių mašinų ekrano kopijas kas sekundę. PĮ gali rūšiuoti analizės įvykius chronologiška seka. PĮ turi galimybę siųsti pranešimus apie identifikuotus įvykius bent šiais protokolais: - syslog (syslog, rsyslog, syslog-ng); - SMTP (informuoti el. paštu). PĮ turi galimybę siųsti pranešimus, aukščiau įvardintais protokolais, apie įvykius naudojant bent šiuos formatus: - tekstinį (angl. text); - JSON; - XML; PĮ geba sugeneruotas ataskaitas patalpinti į struktūrizuotą rezultatų aplankalą, kuriame ataskaitos yra patalpinamos atskirais formatais: html/json/xml/ maec/openIOC PĮ turi galimybę siųsti pranešimus apie atliktą analizę el. paštu.
2.8.	PĮ privalo turėti integracijos galimybę su Virus Total duomenų baze per Rest - API.	PĮ turi integracijos galimybę su Virus Total duomenų baze per Rest - API.
2.9.	Programinės įrangos palaikymo trukmė ne trumpesnė nei 12 mėn.	Programinės įrangos palaikymo trukmė 12 mėn.
2.10.	Programinės įrangos palaikymo sąlygos turi leisti iš gamintojo svetainės parsisiųsti ir naudoti paskutinę programinės įrangos versiją bei atnaujinimus visą licencijos galiojimo laikotarpį.	Programinės įrangos palaikymo sąlygos leidžia iš gamintojo svetainės parsisiųsti ir naudoti paskutinę programinės įrangos versiją bei atnaujinimus visą licencijos galiojimo laikotarpį.
2.11.	Programinės įrangos palaikymo sąlygos turi suteikti programinės įrangos techninės pagalbos paslaugą visą licencijos galiojimo laikotarpį.	Programinės įrangos palaikymo sąlygos suteikia programinės įrangos techninės pagalbos paslaugą visą licencijos galiojimo laikotarpį.

Pastabos:

*Teikdamas siūlomų prekių aprašymą, tiekėjas negali naudoti sąvokų „*Atitinka*“ ar „*Taip*“, o privalo aiškiai apibūdinti siūlomų prekių charakteristikas, priešingu atveju toks pasiūlymas bus pripažintas neatitinkančiu pirkimo dokumentų reikalavimų ir bus atmestas.

** Nurodyti pavadinimai, medžiagų / įrangos gamintojai technologinis procesas, standartas, prekių kilmė, konkretus pavadinimas, ženklas (jei tokią prielaidą galima daryti) yra informacinio pobūdžio ir tiekėjas nėra įpareigojamas siūlyti ir/ar naudoti šių gamintojų produkciją, standartą, procesą (gali naudoti lygiaverčius). Teikdamas pasiūlymą, tiekėjas turi vadovautis šiuo metu galiojančiais normatyvais technologijai, medžiagoms, įrangai bei darbams, atsižvelgti į pirkimo objekto specifiką. Lygiavertiškumo nurodytiems duomenims įrodymo prievolė tenka tiekėjui.

Kartu su pasiūlymu pateikiami šie dokumentai:

Eil. Nr.	**Pateiktų dokumentų pavadinimas**	**Dokumento puslapių skaičius**
1.	Įgaliojimas	1
2.	EBVPD	13

Pasiūlymas galioja iki termino, nustatyto pirkimo dokumentuose.

Ši pasiūlyme nurodyta informacija konfidenciali (*Pirkėjas šios informacijos negali atskleisti tretiesiems asmenims*):

Eil. Nr.	Pateikto dokumento pavadinimas (rekomenduojama pavadinime vartoti žodį „Konfidencialu“)	Dokumentas yra įkeltas šioje CVP IS pasiūlymo lango eilutėje („Prisegti dokumentai“)

Dalyviui nenurodžius, kokia informacija yra konfidenciali, laikoma, kad konfidencialios informacijos pasiūlyme nėra ir vadovaujantis Viešųjų pirkimų tarnybos direktoriaus 2017 m. birželio 19 d. įsakymu Nr. 1S-91 laimėjusio dalyvio pasiūlymas ir su juo pasirašyta sutartis bus viešinama visa apimtimi.

Komercijos direktorius		Darius Dulskas
(Tiekėjo arba jo įgalioto asmens pareigų pavadinimas)	(Parašas)	(Vardas ir pavardė)

Dokumentą elektroniniu parašu pasirašė
DARIUS,DULSKAS
Data: 2020-10-05 07:17:02