UAB "ATEA"
J. Rutkausko g. 6, LT-05132, Vilnius, Lietuva
Tel. 8-37-400036 Faks. 8-37-400050

Nordea Bank Finland Plc Lietuvos skyrius
Banko kodas: 21400
Atsisk. sąskaita: LT032140030001327814
Įm. kodas 122588443
PVM mokėtojo kodas: LT225884413

VšĮ Kėdainių pirminės sveikatos
priežiūros centrui

PASIŪLYMAS
DĖL PROGRAMINĖS ĮRANGOS LICENCIJŲ PIRKIMO

2015 11 05 Nr. KAU_P20151105/01

Kaunas

Tiekėjo pavadinimas	UAB „ATEA“
Įmonės kodas	122588443
Tiekėjo adresas	J. Rutkausko g. 6, LT-05132, Vilnius
Už pasiūlymą atsakingo asmens vardas, pavardė, pareigos	Projektų vadovas Arvydas Monkevičius
Telefono numeris	
Fakso numeris	+370 37 40 00 50
El. pašto adresas	Arvydas.Monkevicius@atea.lt

1. Šiuo pasiūlymu pažymime, kad sutinkame su visomis pirkimo sąlygomis, nustatytomis:
   1) mažos vertės pirkimo apklausos būdu konkurso sąlygose „Programinės įrangos licencijų pirkimas“;
   2) kituose pirkimo dokumentuose (jų paaiškinimuose, papildymuose).
2. Pateikdamas CVP IS priemonėmis pasiūlymą, patvirtinu, kad dokumentų skaitmeninės kopijos ir elektroninėmis priemonėmis pateikti duomenys yra tikri.

Mes siūlome *šias prekes:*

Eil. Nr.	Prekių pavadinimas	Kiekis	Mato vnt.	Vieneto kaina, Eur, be PVM	Vieneto kaina, Eur, su PVM	Kaina Eur su PVM
1.	Antivirusinės apsaugos programos licencija	19	vnt.	23,00	27,83	528,77
2.	Rezervinio kopijavimo ir replikavimo programinės įrangos licencija	1	vnt.	1140,00	1379,40	1379,40
				IŠ VISO (bendra pasiūlymo kaina)		1908,17

Bendra pasiūlymo kaina be PVM 1577,00Eur (*tūkstantis penki šimtai septyniasdešimt septyni Eur, 00 cnt*), o su PVM 1908,17 Eur (*tūkstantis devyni šimtai aštuoni Eur, 17 cnt*).

Iš jų PVM yra 331,17 Eur (*trys šimtai trisdešimt vienas Eur, 17 cnt*).

Siūlomos *prekes* visiškai atitinka pirkimo dokumentuose nurodytus reikalavimus.

Kartu su pasiūlymu pateikiami šie dokumentai:

Eil. Nr.	Pateiktų dokumentų pavadinimas	Dokumento puslapių skaičius
1.	Techninė specifikacija	6
2.	Tiekėjo deklaracija	1

Pasiūlymas galioja iki termino, nustatyto pirkimo dokumentuose.

Direktorius		Raimundas Puskunigis
(Tiekėjo arba jo įgalioto asmens pareigų pavadinimas*)	(Parašas*)	(Vardas ir pavardė*)

PROGRAMINĖS ĮRANGOS LICENCIJŲ TECHNINĖ SPECIFIKACIJA

Eil. Nr.	Komponento pavadinimas	Reikalaujama charakteristika	Siūloma charakteristika, gamintojas, modelis, kodas
1.	**Antivirusinės apsaugos programos licencija – 19 vnt.**		
1.1	Antivirusinės apsaugos programos licencija	19 licencijų atnaujinimas 36 mėnesiams Virtualizuotų tarnybinių tinklo stočių apsaugos programinė įranga. Sistemos paskirtis: • Organizacijai priklausančių virtualizuotų tarnybinių stočių apsauga nuo išorės ir vidinių grėsmių (kompiuteriniai virusai, šnipinėjimo programos, įsilaužimai, informacijos nutekėjimas) Siūlomas apsaugos sprendimas turi apimti: • 10 virtualizuotos tarnybinės stotys. Programinės įrangos versija: • Turi būti siūloma naujausia, gamintojo svetainėje oficialiai paskelbta, programinės įrangos versija. Pagrindinės sistemos funkcijos (komponentai): • Darbo vietų kompiuterių ir serverių apsauga nuo kompiuterinių virusų ir šnipinėjimo programų; • Tarnybinių stočių apsauga nuo įsilaužimų (firewall); • Įsilaužimų prevencijos mechanizmas; • Programų ir aplikacijų paleidimo kontrolė; • Turi gebėti skenavimo metu indeksuoti tarnybinėse stotyse esančias bylas ir praleisti patikrintų bylų skenavimą jeigu jos nėra pakitusios po paskutinio patikrinimo; • Turi turėti galimybę naudoti bendrą tinklinį indeksą, kurio dėka vienoje tarnybinėje stotyje patikrintos bylos nebūtų skanuojamos kitoje tarnybinėje stotyje; • Turi palaikyti virtualizacijos technologijas ir automatiškai atpažinti virtualizuotas tanybines stotis; • Turi būti galimybė sudaryti programų „baltąjį sąrašą“ ir leisti užkraiti tik šiame sąraše esančias programas, visų kitų programų paleidimas būtų draudžiamas. Tarnybinių stočių apsaugos programinės įrangos darbo terpė: • Windows Server 2003 (32bit, 64bit) • Windows Server 2008 (32bit, 64bit) • Windows Server 2012 Gamintojas turi garantuoti palaikymą ir naujų apsaugos programų versijų pateikimą naujoms, techninio aptarnavimo laikotarpiu išleidžiamoms, Microsoft operacinėms sistemoms (serveriams, darbo vietoms) Apsaugos programinė įranga turi būti suderinama su šiomis virtualizacijos terpėmis: • Microsoft Hyper-V; • VmWare vSphere Server (ESXi); • Citrix XenServer. Funkciniai reikalavimai apsaugos nuo kompiuterinių virusų komponentui: Komponento paskirtis: kompiuterių apsauga nuo kompiuterinių virusų ir	SYMANTEC ENDPOINT PROTECTION 12.1 19 licencijų atnaujinimas 36 mėnesiams Virtualizuotų tarnybinių tinklo stočių apsaugos programinė įranga. Sistemos paskirtis: • Organizacijai priklausančių virtualizuotų tarnybinių stočių apsauga nuo išorės ir vidinių grėsmių (kompiuteriniai virusai, šnipinėjimo programos, įsilaužimai, informacijos nutekėjimas) Siūlomas apsaugos sprendimas apima: • 10 virtualizuotos tarnybinės stotys. Programinės įrangos versija: • naujausia, gamintojo svetainėje oficialiai paskelbta, programinės įrangos versija. Pagrindinės sistemos funkcijos (komponentai): • Darbo vietų kompiuterių ir serverių apsauga nuo kompiuterinių virusų ir šnipinėjimo programų; • Tarnybinių stočių apsauga nuo įsilaužimų (firewall); • Įsilaužimų prevencijos mechanizmas; • Programų ir aplikacijų paleidimo kontrolė; • Geba skenavimo metu indeksuoti tarnybinėse stotyse esančias bylas ir praleisti patikrintų bylų skenavimą jeigu jos nėra pakitusios po paskutinio patikrinimo; • Turi galimybę naudoti bendrą tinklinį indeksą, kurio dėka vienoje tarnybinėje stotyje patikrintos bylos nebūtų skanuojamos kitoje tarnybinėje stotyje; • Palaiko virtualizacijos technologijas ir automatiškai atpažįsta virtualizuotas tanybines stotis; • Yra galimybe sudaryti programų „baltąjį sąrašą“ ir leidžia užkrauti tik šiame sąraše esančias programas, visų kitų programų paleidimas būtų draudžiamas. Tarnybinių stočių apsaugos programinės įrangos darbo terpė: • Windows Server 2003 (32bit, 64bit) • Windows Server 2008 (32bit, 64bit) • Windows Server 2012 Gamintojas garantuoja palaikymą ir naujų apsaugos programų versijų pateikimą naujoms, techninio aptarnavimo laikotarpiu išleidžiamoms, Microsoft operacinėms sistemoms (serveriams, darbo vietoms) Apsaugos programinė įranga yra suderinama su šiomis virtualizacijos terpėmis: • Microsoft Hyper-V; • VmWare vSphere Server (ESXi); • Citrix XenServer.

		šnipinėjimo programų. • Įdiegti antivirusinės programinės įrangos moduliai turi apsaugoti savo procesus nuo sustabdymo arba automatiškai juos vėl paleisti, jei šie kokiu nors neleistinu būdu buvo sustabdyti; • Turi gebėti aptikti ir neutralizuoti neautorizuotas programas, kurios bando gauti sisteminę ir konfidencialią informaciją: virusus, kirminus (worms), „rootkits", „Trojos arklius" (Trojans), šnipinėjimo programas (spyware), klaviatūros paspaudimų surinkėjus (key loggers), piktybines reklamines programas (adware, identifikuoti pik-tybines programas (dialers, joke programs, remote access ir hack); • Turi turėti euristinį grėsmių aptikimo mechanizmą; • Turi sugebėti aptikti ir sustabdyti atakas iki virusų aprašų (virus definition) išleidimo (zero-day attacks); • Turi turėti galimybę aptikti grėsmes ir sustabdyti įtartinus procesus, vykstančius kompiuterio operatyvioje atmintyje iki sukeliant jiems žalą, atminties skenavimo metu nutraukti aptiktus procesus, kurie gali sukelti grėsmę sistemos darbui; • Turi turėti lokalaus ir centralizuoto „karantino" pasirinkimo galimybę; • Turi turėti galimybę vykdyti kompiuterio sistemos ir failų skenavimą pagal tvarkaraštį arba inicijavus administratoriaus nurodymu iš valdymo konsolės; • Turi turėti galimybę atlikti išorinių informacijos laikmenų skenavimą; • Siūlomos antivirusinės sistemos gamintojas turi būti sėkmingai išlaikęs bent vieną Virus Bulletin 2012 metų testą VB100 arba lygiavertį; • Turi turėti operatyvaus automatinio atsinaujinimo funkciją; • Turi būti operatyvus ataskaitų formavimas apie rastus virusus į valdymo konsolę. • Komponentas turi būti valdomas iš bendros valdymo konsolės. • Turi būti galimybė uždrausti vartotojams, darbo vietose turintiems administravimo teises, standartinėmis OS priemonėmis sustabdyti antivirusinės programinės įrangos tarnybą. Funkciniai reikalavimai apsaugos nuo įsilaužimų komponentui Komponento paskirtis: kompiuterių apsauga nuo galimų įsilaužimų į sistemą. • Ugniasienė turi apsaugoti nuo nepageidaujamų tinklo išorinių atakų, t.y. pagal nustatytus kriterijus (pagal prievadus (port) ir programas) turi riboti atakos šaltinio prieigą. • Komponentas turi būti valdomas iš bendros valdymo konsolės. Funkciniai reikalavimai įsilaužimų prevencijos komponentui Komponento paskirtis: kompiuterių apsauga nuo galimų įsilaužimų į sistemą.	Funkciniai reikalavimai apsaugos nuo kompiuterinių virusų komponentui: Komponento paskirtis: kompiuterių apsauga nuo kompiuterinių virusų ir šnipinėjimo programų. • Įdiegti antivirusinės programinės įrangos moduliai apsaugo savo procesus nuo sustabdymo arba automatiškai juos vėl paleidžia, jei šie kokiu nors neleistinu būdu buvo sustabdyti; • Geba aptikti ir neutralizuoti neautorizuotas programas, kurios bando gauti sisteminę ir konfidencialią informaciją: virusus, kirminus (worms), „rootkits", „Trojos arklius" (Trojans), šnipinėjimo programas (spyware), klaviatūros paspaudimų surinkėjus (key loggers), piktybines reklamines programas (adware, identifikuoti pik-tybines programas (dialers, joke programs, remote access ir hack); • Turi euristinį grėsmių aptikimo mechanizmą; • Sugeba aptikti ir sustabdyti atakas iki virusų aprašų (virus definition) išleidimo (zero-day attacks); • Turi galimybę aptikti grėsmes ir sustabdyti įtartinus procesus, vykstančius kompiuterio operatyvioje atmintyje iki sukeliant jiems žalą, atminties skenavimo metu nutraukti aptiktus procesus, kurie gali sukelti grėsmę sistemos darbui; • Turi lokalaus ir centralizuoto „karantino" pasirinkimo galimybę; • Turi galimybę vykdyti kompiuterio sistemos ir failų skenavimą pagal tvarkaraštį arba inicijavus administratoriaus nurodymu iš valdymo konsolės; • Turi galimybę atlikti išorinių informacijos laikmenų skenavimą; • Antivirusinės sistemos gamintojas yra sėkmingai išlaikęs bent vieną Virus Bulletin 2012 metų testą VB100; • Turi operatyvaus automatinio atsinaujinimo funkciją; • Yra operatyvus ataskaitų formavimas apie rastus virusus į valdymo konsolę. • Komponentas yra valdomas iš bendros valdymo konsolės. • Yra galimybė uždrausti vartotojams, darbo vietose turintiems administravimo teises, standartinėmis OS priemonėmis sustabdyti antivirusinės programinės įrangos tarnybą. Funkciniai reikalavimai apsaugos nuo įsilaužimų komponentui Komponento paskirtis: kompiuterių apsauga nuo galimų įsilaužimų į sistemą. • Ugniasienė apsaugo nuo nepageidaujamų tinklo išorinių atakų, t.y. pagal nustatytus kriterijus (pagal prievadus (port) ir programas) riboja atakos šaltinio prieigą. • Komponentas yra valdomas iš bendros valdymo konsolės. Funkciniai reikalavimai įsilaužimų

		• Turi turėti HIPS (Host Intrusion Prevention System). • Turi turėti per tinklą gaunamų paketų analizę, palyginti su galimų įsilaužimų scenarijais; • Turi turėti nuolatinį galimų įsilaužimo scenarijų papildymą (atnaujinimą) kartu su virusų aprašais; • Turi turėti kompiuteryje veikiančių procesų stebėjimą, analizę ir blokavimą, jei tipinis procesas bando atlikti sau nebūdingą funkciją (pvz., spausdinimo procesas bando kreiptis į internetą); • Turi turėti potencialiai pavojingų programų, jų instaliacinių paketų identifikavimą kompiuteriuose jų skanavimo metu, galimybę juos ištrinti arba padėti į „karantiną"; • Komponentas turi būti valdomas iš bendros valdymo konsolės. Funkciniai reikalavimai periferinių įrenginių kontrolės komponentui: Komponento paskirtis: kontroliuoti organizacijoje informacijos kopijavimą į išorinius įrenginius, užkirsti kelią žalingų programų patekimui į vidinius tinklus. • Turi turėti galimybę uždrausti naudoti per USB jungiamus išorinius atminties įrenginius (USB atmintines, išorinius diskus, kt.); • Turi turėti galimybę daryti išimtis, pvz., leisti naudotis tik tam tikro aprašyto tipo USB atmintines; • Turi turėti galimybę uždrausti naudoti Bluetooth įrenginių naudojimą; • Komponentas turi būti valdomas iš bendros valdymo konsolės. Funkciniai reikalavimai aplikacijų kontrolės komponentui: Komponento paskirtis: riboti organizacijoje nepageidaujamų programų naudojimą. • Turi turėti galimybę uždrausti darbo vietose naudoti tam tikras programas (pvz., Skype); • Komponentas turi būti valdomas iš bendros valdymo konsolės. Reikalavimai sistemos konfigūracijai ir diegimui • Turi būti galimybė programinę įrangą diegti centralizuotai iš valdymo konsolės, lokaliai iš laikmenos (arba per tinklą) arba per Active Directory Group Policy nustatymus; • Diegimo metu turi būti galimybė pasirinkti kokie komponentai (apsauga nuo virusų, šnipinėjimo programų, ugniasienė, išorinių įrenginių ir aplikacijų kontrolė, prisijungimo prie tinklo kontrolė) bus diegiami į kompiuterį; • Įdiegus į darbo vietos kompiuterį apsaugos sistemą ši neturi reikalauti papildomo konfigūravimo darbų (nustatyti ryšius su valdymo konsole, nurodyti atnaujinimų dislokacijos vietą, derinti kitus nustatymus); • Visi serveriuose esantys agentai turi būti	prevencijos komponentui Komponento paskirtis: kompiuterių apsauga nuo galimų įsilaužimų į sistemą. • Turi HIPS (Host Intrusion Prevention System). • Turi per tinklą gaunamų paketų analizę, palyginti su galimų įsilaužimų scenarijais; • Turi nuolatinį galimų įsilaužimo scenarijų papildymą (atnaujinimą) kartu su virusų aprašais; • Turi kompiuteryje veikiančių procesų stebėjimą, analizę ir blokavimą, jei tipinis procesas bando atlikti sau nebūdingą funkciją (pvz., spausdinimo procesas bando kreiptis į internetą); • Turi potencialiai pavojingų programų, jų instaliacinių paketų identifikavimą kompiuteriuose jų skanavimo metu, galimybę juos ištrinti arba padėti į „karantiną"; • Komponentas yra valdomas iš bendros valdymo konsolės. Funkciniai reikalavimai periferinių įrenginių kontrolės komponentui: Komponento paskirtis: kontroliuoja organizacijoje informacijos kopijavimą į išorinius įrenginius, užkerta kelią žalingų programų patekimui į vidinius tinklus. • Turi galimybę uždrausti naudoti per USB jungiamus išorinius atminties įrenginius (USB atmintines, išorinius diskus, kt.); • Turi galimybę daryti išimtis, pvz., leisti naudotis tik tam tikro aprašyto tipo USB atmintines; • Turi galimybę uždrausti naudoti Bluetooth įrenginių naudojimą; • Komponentas yra valdomas iš bendros valdymo konsolės. Funkciniai reikalavimai aplikacijų kontrolės komponentui: Komponento paskirtis: riboja organizacijoje nepageidaujamų programų naudojimą. • Turi galimybę uždrausti darbo vietose naudoti tam tikras programas (pvz., Skype); • Komponentas yra valdomas iš bendros valdymo konsolės. Reikalavimai sistemos konfigūracijai ir diegimui • Turi galimybė programinę įrangą diegti centralizuotai iš valdymo konsolės, lokaliai iš laikmenos (arba per tinklą) arba per Active Directory Group Policy nustatymus; • Diegimo metu yra galimybė pasirinkti kokie komponentai (apsauga nuo virusų, šnipinėjimo programų, ugniasienė, išorinių įrenginių ir aplikacijų kontrolė, prisijungimo prie tinklo kontrolė) bus diegiami į kompiuterį; • Įdiegus į darbo vietos kompiuterį apsaugos sistemą ši nereikalauja papildomo konfigūravimo darbų (nustatyti ryšius su valdymo konsole, nurodyti atnaujinimų dislokacijos vietą, derinti

		valdomi iš bendros centralizuotos konsolės. Funkciniai reikalavimai valdymo konsolei: • Konsolėje turi matytis visi sistemos agentus turintys kompiute riai, jų statusas ir bendra informacija; • Turi turėti centralizuoto „karantino" serveryje funkcionalumą; • Turi turėti centralizuotą bendros politikos (politikų) nustatymą visiems programinės įrangos klientams; • Turi leisti keisti pranešimo (alert) apie aptiktą grėsmę turinį; • Turi būti centralizuotai ir automatiškai atnaujinama klientų programinės dalies ir virusų parašų bazė, nereikalaujant sistemos įkrovimo iš naujo; • Turi būti suderinama su Microsoft Active Directory (informacijos apie vartotojus ir kompiuterius sinchronizavimas); • Turi turėti funkcionalumą vartotojų grupėms nustatyti skirtingus klientinės dalies parametrų nustatymus, taip kuriant pasirinktai grupei bendrą saugumo taisyklių rinkinį; • Turi turėti galimybę automatiniu būdu (elektroniniu paštu) valdymo serverio administratorių informuoti apie darbo vietoje įvykusį incidentą; • Turi turėti funkcionalumą nustatyti administravimo taisykles nešiojamiems kompiuteriams, kurie nėra pastoviai prijungti prie vidinio tinklo ir nepasiekia valdymo serverio; • Turi turėti funkcionalumą skenuoti kompiuterių tinklą ir rasti kompiuterius, kurie neturi jokios antivirusinės programinės įrangos; • Turi būti funkcionalumas fiksuoti pranešimus apie sisteminius įvykius ir incidentus, įvykusius klientinėje darbo vietoje ir persiųsti juos į centralizuotą valdymo serverį; • Turi turėti ataskaitų sudarymo įvairiais pjūviais funkcionalumą ir grafinių ataskaitų atvaizdavimą; • Turi turėti galimybę vieną valdymo serverį naudoti dviejų nepriklausomų padalinių kompiuerių valdymui, kai naudojamos atskiros licencijos ir šias organizacijas administruoja skirtingi žmonės, realizuojant šį funkcionalumą tokiu būdu, kad valdymo konsolėje organizacijos viena kitai būtų nematomos ir jos naudotų tik joms skirtas licencijas; • Turi turėti galimybę paskirti pasirinktus organizacijoje esančius kompiuterius atnaujinimų ir diegimo paketų retransliavimui naudojant tik kompiuteriuose jau įdiegta antivirusinę programą ir nediegiant papildomų administravimo serverių. Atnaujinimai ir palaikymas Pateikiamoms licencijoms turi būti užtikrinamas 3(trijų) metų gamintojo palaikymas nuo Programinės įrangos pristatymo Perkančiajai	kitus nu-statymus); • Visi serveriuose esantys agentai yra valdomi iš bendros centralizuotos konsolės. Funkciniai reikalavimai valdymo konsolei: • Konsolėje matosi visi sistemos agentus turintys kompiute riai, jų statusas ir bendra informacija; • Turi centralizuoto „karantino" serveryje funkcionalumą; • Turi centralizuotą bendros politikos (politikų) nustatymą visiems programinės įrangos klientams; • Leidžia keisti pranešimo (alert) apie aptiktą grėsmę turinį; • Yra centralizuotai ir automatiškai atnaujinama klientų programinės dalies ir virusų parašų bazė, nereikalaujanti sistemos įkrovimo iš naujo; • Yra suderinama su Microsoft Active Directory (informacijos apie vartotojus ir kompiuterius sinchronizavimas); • Turi funkcionalumą vartotojų grupėms nustatyti skirtingus klientinės dalies parametrų nustatymus, taip kuriant pasirinktai grupei bendrą saugumo taisyklių rinkinį; • Turi galimybę automatiniu būdu (elektroniniu paštu) valdymo serverio administratorių informuoti apie darbo vietoje įvykusį incidentą; • Turi funkcionalumą nustatyti administravimo taisykles nešiojamiems kompiuteriams, kurie nėra pastoviai prijungti prie vidinio tinklo ir nepasiekia valdymo serverio; • Turi funkcionalumą skenuoti kompiuterių tinklą ir rasti kompiuterius, kurie neturi jokios antivirusinės programinės įrangos; • Yra funkcionalumas fiksuoti pranešimus apie sisteminius įvykius ir incidentus, įvykusius klientinėje darbo vietoje ir persiųsti juos į centralizuotą valdymo serverį; • Turi ataskaitų sudarymo įvairiais pjūviais funkcionalumą ir grafinių ataskaitų atvaizdavimą; • Turi galimybę vieną valdymo serverį naudoti dviejų nepriklausomų padalinių kompiuerių valdymui, kai naudojamos atskiros licencijos ir šias organizacijas administruoja skirtingi žmonės, realizuojant šį funkcionalumą tokiu būdu, kad valdymo konsolėje organizacijos viena kitai būtų nematomos ir jos naudotų tik joms skirtas licencijas; • Turi galimybę paskirti pasirinktus organizacijoje esančius kompiuterius atnaujinimų ir diegimo paketų retransliavimui naudojant tik kompiuteriuose jau įdiegta antivirusinę programą ir nediegiant papildomų administravimo serverių. Atnaujinimai ir palaikymas pateikiamoms licencijoms yra užtikrinamas 3(trijų) metų

		organizacijai dienos, užtikrinantis teisę šiuo laikotarpiu be papildomo mokesčio: • Operatyviai gauti naujausius virusų aprašus (virus definitions), šnipinėjimo programų aprašus (anti-spyware definitions); • Gauti visus sistemos programų atnaujinimus, pataisymus ir naujas versijas; • Gauti technines konsultacijas ir pagalbą; • Gauti technines konsultacijas ir pagalbą internetu; • Klientinės dalies programinė įranga privalo parsisiųsti atnaujinimus tiesiai iš gamintojo atnaujinimų serverio, centralizuoto valdymo serverio arba kt. klientų; • Programinės įrangos gamintojas privalo turėti internetinį puslapį, kuriame būtų žalingų programų ir jų sukeliamų pažeidžiamumų duomenų bazė, informacija apie produktus; • Standartinės aptarnavimo sąlygos vykdomos pagal licencinės sutarties sąlygas.	gamintojo palaikymas nuo programinės įrangos pristatymo perkančiajai organizacijai dienos, užtikrinantis teisę šiuo laikotarpiu be papildomo mokesčio: • Operatyviai gauti naujausius virusų aprašus (virus definitions), šnipinėjimo programų aprašus (anti-spyware definitions); • Gauti visus sistemos programų atnaujinimus, pataisymus ir naujas versijas; • Gauti technines konsultacijas ir pagalbą; • Gauti technines konsultacijas ir pagalbą internetu; • Klientinės dalies programinė įranga parsisiunčia atnaujinimus tiesiai iš gamintojo atnaujinimų serverio, centralizuoto valdymo serverio arba kt. klientų; • Programinės įrangos gamintojas turi internetinį puslapį, kuriame yra žalingų programų ir jų sukeliamų pažeidžiamumų duomenų bazė, informacija apie produktus; • Standartinės aptarnavimo sąlygos vykdomos pagal licencinės sutarties sąlygas.
2.	**Rezervinio kopijavimo ir replikavimo licencija – 1 vnt.**		
2.1	Licencijavimo būdas ir licencijų kiekis-1 vnt.	Per fizinį procesorių, nepriklausomai nuo procesoriaus branduolių skaičiaus. Vardinė (-ės) licencija (-os), leidžianti (-čios) naudoti programinę įrangą su bet kuria Perkančiosios organizacijos fizine tarnybine stotimi. Turi būti pateikta licencija (-os) 2 procesoriams (angl. socket). Licencija turi neriboti replikuojamų, kopijuojamų ir atstatomų virtualių mašinų skaičiaus ar duomenų kiekio.	Veeam Backup Essentials Enterprise Per fizinį procesorių, nepriklausomai nuo procesoriaus branduolių skaičiaus. Vardinė (-ės) licencija (-os), leidžianti (-čios) naudoti programinę įrangą su bet kuria perkančiosios organizacijos fizine tarnybine stotimi. Yra pateikta licencija (-os) 2 procesoriams (angl. socket). Licencija neriboja replikuojamų, kopijuojamų ir atstatomų virtualių mašinų skaičiaus ar duomenų kiekio.
	Palaikomos virtualios aplinkos	Turi būti pateiktos licencijos užtikrinančios rezervinį kopijavimą, replikavimą ir atstatymą siūlomos virtualizacijos platformos tarnybinėms stotims. Virtualioje aplinkoje veikimas turi būti užtikrinamas, neįdiegiant agentų (angl. „agent less“) į virtualias mašinas ar virtualizacijos platformos tarnybines stotis.	Yra pateiktos licencijos užtikrinančios rezervinį kopijavimą, replikavimą ir atstatymą siūlomos virtualizacijos platformos tarnybinėms stotims. Virtualioje aplinkoje veikimas yra užtikrinamas, neįdiegiant agentų (angl. „agent less“) į virtualias mašinas ar virtualizacijos platformos tarnybines stotis.
	Funkcionalumas	Turi būti pateiktos visos reikalingos licencijos, užtikrinančios žemiau nurodytus funkcionalumus: • Daryti/ atkurti virtualių mašinų rezervines duomenų kopijas, jų nestabdant; • Asinchroniškai replikuoti virtualias mašinas į iš anksto aprašytą duomenų laikmeną ar nutolusį duomenų centrą; • Turi atstatyti virtualias mašinas į kitą virtualizuotą tarnybinę stotį; • Turi atstatyti virtualią mašiną tiesiai iš rezervinių duomenų kopijos esančios rezervinėje duomenų saugykloje, nekopijuojant duomenų į darbinę duomenų saugyklą;	Yra pateiktos visos reikalingos licencijos, užtikrinančios žemiau nurodytus funkcionalumus: • Daro/ atkuria virtualių mašinų rezervines duomenų kopijas, jų nestabdant; • Asinchroniškai replikuoja virtualias mašinas į iš anksto aprašytą duomenų laikmeną ar nutolusį duomenų centrą; • Atstato virtualias mašinas į kitą virtualizuotą tarnybinę stotį; • Atstato virtualią mašiną tiesiai iš rezervinių duomenų kopijos esančios rezervinėje duomenų saugykloje, nekopijuojant duomenų į darbinę duomenų saugyklą; Palaikomas duomenų kopijavimas iš LAN

		Palaikomas duomenų kopijavimas iš LAN ir tiesiogiai iš SAN tinklo.	ir tiesiogiai iš SAN tinklo.
	Duomenų išdubliavimo (atsarginių kopijų darymo būdas), versijavimo užtikrinimas	Turi turėti rezervinių duomenų kopijų išdubliavimo, kompresijos ir versijavimo funkcionalumą, turi būti pateiktos visos tam reikalingos licencijos.	Turi rezervinių duomenų kopijų išdubliavimo, kompresijos ir versijavimo funkcionalumą, yra pateiktos visos tam reikalingos licencijos.
	Rašymas į juostinius įrenginius ir archyvavimas	Turi būti realizuotas centralizuotas automatinis rezervinis kopijavimas pagal nustatytą kalendorių (angl. „schedule"), automatinis duomenų kopijavimas iš diskų į juostinius įrenginius, juostų bibliotekas ir virtualias juostų bibliotekas. Turi būti užtikrintas pilnas virtualių mašinų ir jų atstatymo taškų matomumas juostose.	Yra realizuotas centralizuotas automatinis rezervinis kopijavimas pagal nustatytą kalendorių (angl. „schedule"), automatinis duomenų kopijavimas iš diskų į juostinius įrenginius, juostų bibliotekas ir virtualias juostų bibliotekas. Yra užtikrintas pilnas virtualių mašinų ir jų atstatymo taškų matomumas juostose.
	Paieškos funkcionalumas	Turi užtikrinti rezervinių duomenų kopijų indeksavimą bei paieškos funkciją visoje rezervinių duomenų kopijų bibliotekoje.	Užtikrina rezervinių duomenų kopijų indeksavimą bei paieškos funkciją visoje rezervinių duomenų kopijų bibliotekoje.
	Atkūrimo užtikrinimas	Turi būti realizuotas funkcionalumas automatiškai patikrinti kiekvieną rezervinę duomenų kopiją po jos sukūrimo (turi automatiškai paleisti virtualią mašiną tiesiai iš rezervinės kopijos failo, atlikti iš anksto nustatyto scenarijaus veiksmus bei išsiųsti ataskaitą administratoriui) ir garantuoti duomenų atkūrimą (angl. „recoverability") į tą pačią būseną (kai buvo sukurta rezervinė kopija).	Yra realizuotas funkcionalumas automatiškai patikrinti kiekvieną rezervinę duomenų kopiją po jos sukūrimo (automatiškai paleidžia virtualią mašiną tiesiai iš rezervinės kopijos failo, atlieka iš anksto nustatyto scenarijaus veiksmus bei išsiunčia ataskaitą administratoriui) ir garantuoja duomenų atkūrimą (angl. „recoverability") į tą pačią būseną (kai buvo sukurta rezervinė kopija).
	Pasikeitusių blokų stebėsena	Turi turėti „Change block tracking" funkcionalumą.	Turi „Change block tracking" funkcionalumą.
	Pasikeitimų kopijavimas	Turi palaikyti pasikeitimų atsarginį kopijavimą (angl. „Incremental backup").	Palaiko pasikeitimų atsarginį kopijavimą (angl. „Incremental backup").
	Individualių objektų atstatymas	Turi palaikyti individualių objektų ir failų atstatymą iš MS Exchange, SharePoint, SQL, Active Directory ir kito tipo virtualių mašinų, neatstatant visos virtualios mašinos.	Palaiko individualių objektų ir failų atstatymą iš MS Exchange, SharePoint, SQL, Active Directory ir kito tipo virtualių mašinų, neatstatant visos virtualios mašinos.
	Valdymo centras	Turi turėti vieną centralizuotą valdymo konsolę (visoms rezervinėms duomenų kopijoms ir replikoms tvarkyti, administruoti ir valdyti). Turi centralizuotai valdyti daugiau nei vieną rezervinio kopijavimo tarnybinę stotį iš vienos centralizuotos valdymo konsolės. Turi valdyti Hyper-V ir VMware arba lygiavertes virtualias infrastruktūras iš vienos centralizuotos valdymo konsolės.	Turi vieną centralizuotą valdymo konsolę (visoms rezervinėms duomenų kopijoms ir replikoms tvarkyti, administruoti ir valdyti). Centralizuotai valdo daugiau nei vieną rezervinio kopijavimo tarnybinę stotį iš vienos centralizuotos valdymo konsolės. Valdo Hyper-V ir VMware virtualias infrastruktūras iš vienos centralizuotos valdymo konsolės.
	Palaikymas ir versijų naujinimas	Turi būti pateiktas gamintojo teikiamas programinės įrangos licencijų palaikymas, aptarnavimas ir nemokamas naujų versijų pateikimas 1 metams.	Yra pateiktas gamintojo teikiamas programinės įrangos licencijų palaikymas, aptarnavimas ir nemokamas naujų versijų pateikimas 1 metams.

UAB "ATEA"
J. Rutkausko g. 6, LT-05132 Vilnius, Lietuva
Tel. (8-5) 2397836 Faks. (8-5) 2397831

Nordea Bank Finland Plc Lietuvos skyrius
Banko kodas: 21400
Atsisk. sąskaita: LT032140030001327814
Įm. kodas 122588443
PVM mokėtojo kodas: LT225884413

VšĮ Kėdainių Pirminės sveikatos
priežiūros centrui

TIEKĖJO DEKLARACIJA
2015 m. lapkričio 4 d. Nr. KAU_P20151104/03
Kaunas

1. Aš, direktorius, Raimundas Puskunigis, tvirtinu, kad mano vadovaujama UAB „ATEA", dalyvaujanti VšĮ Kėdainių pirminės sveikatos priežiūros centro atliekamame mažos vertės apklausos būdu konkurse „**PROGRAMINĖS ĮRANGOS LICENCIJŲ PIRKIMAS**", pirkimo numeris 251456 (CVP IS pirkimo numeris 251456) elektroninėmis priemonėmis, paskelbtomis „VšĮ Kėdainių pirminės sveikatos priežiūros centro supaprastintų viešųjų pirkimų taisyklėmis", nėra su kreditoriais sudaręs taikos sutarties, sustabdęs ar apribojęs savo veiklos, nesiekia priverstinio likvidavimo procedūros ar susitarimo su kreditoriais, taip pat nėra padaręs rimto profesinio pažeidimo (profesinės etikos pažeidimo arba konkurencijos, darbo, darbuotojų saugos ir sveikatos, aplinkosaugos teisės aktų pažeidimo), kai nuo tiekėjo pripažinimo nesilaikančiu profesinės etikos normų momento praėjo mažiau kaip vieni metai arba už kurį tiekėjui (fiziniam asmeniui) yra paskirta administracinė nuobauda arba tiekėjui (juridiniam asmeniui) – ekonominė sankcija, nustatyta Lietuvos Respublikos įstatymuose kai nuo sprendimo, kuriuo buvo paskirta ši sankcija, įsiteisėjimo dienos praėjo mažiau kaip vieni metai, o už Lietuvos Respublikos konkurencijos įstatymo 5 straipsnio pažeidimą tiekėjui, kuris yra juridinis asmuo, yra paskirta ekonominė sankcija, kai nuo sprendimo, kuriuo buvo paskirta ši sankcija įsiteisėjimo dienos praėjo mažiau kaip trys metai.

2. Man žinoma, kad, jeigu mano pateikta deklaracija yra melaginga, vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymo 39 straipsnio 2 dalies 1 punktu (Žin., 1996, Nr. 84-2000; 2006, Nr. 4-102; 2008, Nr. 81-3179) pateiktas pasiūlymas bus atmestas.

3. Tiekėjas už deklaracijoje pateiktos informacijos teisingumą atsako įstatymų nustatyta tvarka.

4. Jeigu viešajame pirkime dalyvauja ūkio subjektų grupė, deklaraciją pildo kiekvienas ūkio subjektas.

Direktorius		Raimundas Puskunigis
(Deklaraciją sudariusio asmens pareigų pavadinimas)	(Parašas)	(Vardas ir pavardė)

*Pastaba. Jeigu perkančioji organizacija pirkimą atlieka CVP IS priemonėmis, šis dokumentas teikiamas pasirašytas saugiu elektroniniu parašu. Tais atvejais, kai pirkimo dokumentuose nustatyta, kad visas pasiūlymas pasirašomas saugiu elektroniniu parašu, šio dokumento atskirai pasirašyti neprivaloma.