Uniwersyteckie Centrum Okulistyki i Onkologii
Samodzielny Publiczny Szpital Kliniczny
Śląskiego Uniwersytetu Medycznego w Katowicach
40-514 Katowice ul. Ceglana 35

Znak sprawy: D/ZP/381/44B/14

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA DOT. PRZETARGU NIEOGRANICZONEGO O WARTOŚCI SZACUNKOWEJ NIEPRZEKRACZAJĄCEJ KWOTY OKREŚLONEJ W PRZEPISACH WYDANYCH NA PODSTAWIE ART. 11 UST. 8 USTAWY Z DNIA 29 STYCZNIA 2004 R. PRAWO ZAMÓWIEŃ PUBLICZNYCH (Dz.U.2013.907 j.t. z późn. zm.), na

udzielenie licencji oraz wdrożenie oprogramowania antywirusowego

Zamawiający:
Uniwersyteckie Centrum Okulistyki i Onkologii Samodzielny Publiczny Szpital Kliniczny Śląskiego Uniwersytetu Medycznego w Katowicach
40-514 Katowice, ul. Ceglana 35
NIP: 954-22-74-017 Regon: 001325767
Tel. 32 / 358-12-00 lub 32/358-13-32 fax. 32 251-84-37 lub 32/358-14-32

II. TRYB UDZIELENIA ZAMÓWIENIA:
Postępowanie prowadzone będzie w trybie przetargu nieograniczonego.

III. PRZEDMIOT ZAMÓWIENIA-
Dostawa oprogramowania antywirusowego w tym :
- 234 licencji na oprogramowanie antywirusowe do stacji roboczych łącznie z firewallem
- konsoli wraz z wdrożeniem do centralnego zarządzania oprogramowaniem (w przypadku zaoferowania oprogramowania innego niż posiadane dotychczas przez Zamawiającego).

Szczegółowy opis wymagań i parametrów technicznych opisano w załączniku nr 4 do siwz.

IV. WYMAGANY TERMIN REALIZACJI ZAMÓWIENIA:
Wykonawca w terminie 10 dni od daty podpisania umowy udzieli Zamawiającemu licencji i wdroży oprogramowanie na 234 stacjach roboczych w siedzibie Zamawiającego oraz przeszkoli administratora Zamawiającego.
W pozostałym zakresie Wykonawca zapewni administratorowi Zamawiającego wsparcie telefoniczne dotyczące konfiguracji oraz rozwiązywania problemów z oprogramowaniem dla stacji roboczych i serwerów w okresie 12 miesięcy od daty podpisania umowy.

V. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ OPIS SPOSOBU DOKONYWANIA OCENY SPEŁNIANIA TYCH WARUNKÓW :
1. O udzielenie zamówienia mogą ubiegać się wykonawcy którzy spełniają warunki dotyczące
- posiadania uprawnień do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania
- posiadania wiedzy i doświadczenia
- dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia
  Za spełniających ten warunek Zamawiający uzna Wykonawców, którzy przedstawią wykaz osób realizujących przedmiot zamówienia tj. minimum jednego pracownika do przeprowadzenia wdrożenia i szkolenia , posiadającego właściwy certyfikat wydany przez producenta oprogramowania lub dystrybutora.
- sytuacji ekonomicznej i finansowej

2. Ponadto o udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:
- nie podlegają wykluczeniu z postępowania o udzielenie zamówienia (art. 24 ust. 1 ustawy Pzp)
- złożą ofertę, której treść odpowiada treści niniejszej Specyfikacji istotnych warunków zamówienia.

3. Wykonawca może polegać na wiedzy i doświadczeniu, potencjale technicznym, osobach zdolnych do wykonania zamówienia lub zdolnościach finansowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nimi stosunków. Wykonawca w takiej sytuacji zobowiązany jest udowodnić zamawiającemu, iż będzie dysponował zasobami niezbędnymi do realizacji zamówienia, w szczególności przedstawiając w tym celu pisemne zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na okres korzystania z nich przy wykonywaniu zamówienia.
4. Ocena spełniania warunków zostanie dokonana na podstawie przedłożonych dokumentów i oświadczeń opisanych w pkt VI siwz. według formuły spełnia/nie spełnia.

VI. WYKAZ OSWIADCZEŃ LUB DOKUMENTÓW , JAKIE MAJĄ DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU .
1. Dla potwierdzenia spełnienia warunków udziału w postępowaniu opisanych w pkt. V.1 siwz - Wykonawca dołączy do oferty oświadczenie zawarte w załączniku nr 2 do SIWZ.
2. Wykaz osób realizujących przedmiot zamówienia tj. minimum jednego pracownika do przeprowadzenia wdrożenia i szkolenia , posiadającego właściwy certyfikat wydany przez producenta oprogramowania lub dystrybutora .Posiadanie właściwych certyfikatów należy udokumentować kopią dołączoną do oferty.
3. W celu wykazania braku podstaw do wykluczenia z postępowania o udzielenie zamówienia w okolicznościach o których mowa w art. 24 ust.1 ustawy Wykonawca dołączy do oferty :

a) oświadczenie o braku podstaw do wykluczenia – załącznik nr 2 do SIWZ
b) aktualny odpis z właściwego rejestru, jeżeli odrębne przepisy wymagają wpisu do rejestru, w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust. 1 pkt 2 ustawy wystawiony

nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert, a w stosunku do osób fizycznych oświadczenia w zakresie art. 24 ust. 1 pkt 2 ustawy.

3. Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej stosuje się odpowiednio § 4 rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2009 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy oraz form, w jakich te dokumenty mogą być składane (Dz. U. 2009 r. nr 226 poz. 1817).
4. Zamawiający wezwie Wykonawców, którzy w określonym terminie nie złożyli wymaganych oświadczeń lub dokumentów, lub którzy nie złożyli pełnomocnictw, albo którzy złożyli wymagane oświadczenia i dokumenty zawierające błędy lub którzy złożyli wadliwe pełnomocnictwa, do ich złożenia w wyznaczonym terminie, chyba że mimo ich złożenia oferta Wykonawcy podlega odrzuceniu albo konieczne będzie unieważnienie postępowania.
5. Złożone na wezwanie Zamawiającego oświadczenia i dokumenty powinny potwierdzić spełnienie przez Wykonawcę warunków udziału w postępowaniu oraz spełnienie wymagań określonych przez Zamawiającego, nie później niż w dniu, w którym upłynął termin składania ofert.

VIII. INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ LUB DOKUMENTÓW, A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI.

1. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert pod warunkiem ,że wniosek o wyjaśnienie treści specyfikacji wpłynie do Zamawiającego nie później niż do końca dnia , w którym upływa połowa wyznaczonego terminu składania ofert. Jeżeli wniosek o wyjaśnienie treści specyfikacji wpłynie po upływie terminu składania wniosku, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania .
2. Oświadczenia, wnioski, zawiadomienia oraz informacje zamawiający i wykonawcy przekazują pisemnie, faksem lub drogą elektroniczną. Jeżeli zamawiający lub wykonawca przekazuje oświadczenia, wnioski, zawiadomienia oraz informacje faxem lub drogą elektroniczną, każda ze stron na żądanie drugiej niezwłocznie potwierdza fakt ich otrzymania.
3. Osoby uprawnione do porozumiewania się z wykonawcami: Andrzej Rechowicz, Dział Zamówień Publicznych, pok. E057, tel. 32 3581-332, faks 32 3581 -432; e-mail zp@szpitalceglana.pl, w godzinach pracy od poniedziałku do piątku godz. 7.25 – 15.00.

IX.WADIUM

Zamawiający nie wymaga wniesienia wadium.

X.TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca jest związany ofertą przez okres 30 dni.
2. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
3. Wykonawca samodzielnie lub na wniosek zamawiającego może przedłużyć termin związania ofertą, z tym, że Zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni.

XI. OPIS SPOSOBU PRZYGOTOWYWANIA OFERTY

1. Wykonawca ponosi wszelkie koszty przygotowania i złożenia oferty.
2. Każdy wykonawca może złożyć tylko jedną ofertę .
3. Ofertę sporządza się w języku polskim z zachowaniem formy pisemnej pod rygorem nieważności.
4. Dokumenty sporządzone w języku obcym muszą być złożone wraz z tłumaczeniem na język polski potwierdzonym za zgodność z oryginałem przez wykonawcę (osobę uprawnioną/ osoby uprawnione do reprezentowania wykonawcy)
5. Zamawiający wymaga, załączenia dokumentów sporządzonych zgodnie z załącznikami do specyfikacji istotnych warunków zamówienia w pełnym brzmieniu. tj:

a) Wypełniony czytelnie, podpisany i opieczętowany przez osobę uprawnioną/ osoby uprawnione do reprezentowania wykonawcy formularz ofertowy według druku stanowiącego załącznik nr 1 niniejszej specyfikacji.
b) Podpisany i opieczętowany przez osobę uprawnioną / osoby uprawnione do reprezentowania wykonawcy formularz oświadczeń wykonawcy według druku stanowiącego załącznik nr 2 niniejszej specyfikacji.
c) Wypełniony, podpisany i opieczętowany przez osobę uprawnioną/ osoby uprawnione do reprezentowania wykonawcy - szczegółowy opis parametrów technicznych załącznik nr 3
d) Wypełniony, podpisany i opieczętowany przez osobę uprawnioną/ osoby uprawnione do reprezentowania wykonawcy - wykaz osób biorących udział w realizacji zamówienia – załącznik nr 4

e) Wypełniony, podpisany i opieczętowany przez osobę uprawnioną/ osoby uprawnione do reprezentowania wykonawcy formularz cenowy zawierający wyszczególnienie asortymentowe i ilościowe stanowiącym załącznik nr 5
f) Załączenie do oferty wymaganych przez Zamawiającego dokumentów i oświadczeń wyszczególnionych w pkt. VI

6. Dokumenty określone w pkt. VI winny być przedstawione w formie oryginałów albo poświadczonych za zgodność z oryginałem przez wykonawcę (osobę uprawnioną/ osoby uprawnione do reprezentowania wykonawcy) kserokopii.
7. W przypadku udzielenia pełnomocnictwa do reprezentacji Wykonawcy wymagane jest złożenie oryginału dokumentu lub czytelnej, wyraźnej kserokopii poświadczonej za zgodność z oryginałem
8. Kwestię składania dokumentów przez wykonawców mających siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej reguluje § 4 rozporządzenia Prezesa Rady Ministrów z dnia 19 lutego 2013 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy oraz form, w jakich te dokumenty mogą być składane.
9. Ofertę należy złożyć w zamkniętej kopercie gwarantującej zachowanie w poufności jej treści oraz zabezpieczenie jej nienaruszalności do terminu otwarcia ofert
10. Koperta powinna być zaadresowana według poniższego wzoru :

„ Nazwa , adres Wykonawcy
.....
Uniwersyteckie Centrum Okulistyki i Onkologii w Katowicach
40-514 Katowice, ul. Ceglana 35
„Oferta na dostawę oprogramowania antywirusowego
– Nie otwierać przed 19.05.2014 godz.10.30"

11. Wykonawca może wprowadzić zmiany do złożonej oferty bądź wycofać ofertę pod warunkiem , że zamawiający otrzyma pisemne powiadomienie o wprowadzeniu zmian bądź wycofaniu przed upływem terminu składania ofert – w sposób analogiczny do sposobu złożenia oferty.
12. Zamawiający żąda wskazania przez wykonawcę w ofercie części zamówienia, której wykonanie powierzy podwykonawcom.
13. Wszelkie poprawki lub zmiany w tekście oferty muszą być parafowane własnoręcznie przez osobę podpisującą ofertę.

XII. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT

Ofertę należy złożyć w zamkniętej kopercie gwarantującej zachowanie w poufności jej treści oraz zabezpieczenie jej nienaruszalności do terminu otwarcia ofert. Ofertę należy złożyć w Uniwersyteckim Centrum Okulistyki i Onkologii w Katowicach przy ul. Ceglanej 35, w sekretariacie pokój D 022. W przypadku złożenia oświadczenia zgodnie z art. 8 ust. 3 ustawy Prawo zamówień publicznych, oświadczenia i zaświadczenia zawierające informacje stanowiącą tajemnicę przedsiębiorstwa powinny być umieszczone w odrębnej kopercie oznakowanej literką „B"

Termin składania ofert upływa w dniu 19 maja 2014 r. o godz.10.00.
Oferty złożone po terminie będą zwrócone bez otwierania.

Otwarcie ofert nastąpi w Uniwersyteckim Centrum Okulistyki i Onkologii w Katowicach przy ul. Ceglanej 35 w pokoju E 057 w dniu 19 maja 2014 r. o godz. 10.30.

XIII. OPIS SPOSOBU OBLICZENIA CENY

1. Cena ma być wyrażona w złotych polskich i musi uwzględniać wszystkie wymagania niniejszej specyfikacji istotnych warunków zamówienia tj. obejmować wszelkie koszty, jakie poniesie Wykonawca z tytułu należytej oraz zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia.
2. Cenę netto i brutto oraz należny podatek VAT należy podać z dokładnością do dwóch miejsc po przecinku.
3. Obowiązującą formą zapłaty za realizację przedmiotu zamówienia będzie wynagrodzenie ryczałtowe, które nie będzie podlegać waloryzacji.

XIV. OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJACY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY, WRAZ Z PODANIEM ZNACZENIA TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

Jedynym kryterium oceny ofert jest cena za realizację całości zamówienia – 100%.

Sposób obliczania liczby punktów badanej oferty za cenę:
C min. – cena minimalna spośród ocenianych ofert
Cn – cena badanej oferty
100 – stały współczynnik
(Cmin / Cn) x 100 x 100% = ilość punktów badanej oferty

XV. INFORMACJE O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

1. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający jednocześnie zawiadomi Wykonawców, którzy złożyli oferty o:
   - wyborze najkorzystniejszej oferty, podając nazwę (firmę), albo imię i nazwisko, siedzibę albo adres zamieszkania i adres wykonawcy, którego ofertę wybrano oraz uzasadnienie jej wyboru oraz nazwy (firmy) , albo imiona i nazwiska, siedziby albo miejsca zamieszkania i adresy wykonawców, którzy złożyli oferty, a także punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację
   - wykonawcach, których oferty zostały odrzucone, podając uzasadnienie faktyczne i prawne,
   - wykonawcach, którzy zostali wykluczeni z postępowania o udzielenie zamówienia podając uzasadnienie faktyczne i prawne.
   - terminie, określonym zgodnie z art. 94 ust. 1 lub 2 ustawy Pzp, po którego upływie umowa w sprawie zamówienia publicznego może być zawarta.
2. Zawiadomienie o wyborze najkorzystniejszej oferty zamawiający niezwłocznie umieści na stronie internetowej www.klinika.katowice.pl oraz w miejscu publicznie dostępnym w swojej siedzibie.
3. Zamawiający zawrze umowę w sprawie zamówienia publicznego, z zastrzeżeniem art. 183 ustawy Pzp, z wybranym wykonawcą w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty faksem lub drogą elektroniczną, albo 10 dni – jeżeli zostało przesłane w inny sposób, na warunkach będących istotnymi postanowieniami, a stanowiącymi wzór umowy – załącznik nr 5 lub nr 5a do niniejszej specyfikacji. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem ww. terminów jeżeli w postępowaniu złożono tylko jedną ofertę, a także, gdy w postępowaniu nie odrzucono żadnej oferty oraz nie wykluczono żadnego wykonawcy. Miejsce i termin podpisania umowy zamawiający wskaże wybranemu w wyniku niniejszego postępowania wykonawcy. Jeżeli wybrana oferta została złożona przez wykonawców o których mowa w art. 23 Prawa zamówień publicznych Zamawiający może żądać przed zawarciem umowy w sprawie niniejszego zamówienia umowy regulującej współpracę tych wykonawców.

XV. POZOSTAŁE REGUŁY POSTĘPOWANIA

1. Zamawiający nie przewiduje udzielenia zamówień uzupełniających, o których mowa w art. 67 ust. 1 pkt 7 Prawa zamówień publicznych.
2. Zamawiający nie dopuszcza możliwości składania ofert wariantowych.
3. Zamawiający nie przewiduje przeprowadzenia aukcji elektronicznej, nie ustanawia dynamicznego systemu zakupów oraz nie zamierza zawrzeć umowy ramowej.
4. Termin płatności – do 30 dni od dnia otrzymania faktury za każdą dostarczoną partię przedmiotu zamówienia.
5. Do spraw nieuregulowanych w niniejszej specyfikacji istotnych warunków zamówienia mają zastosowanie przepisy ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2007 r. Nr 223 poz. 1655 z późn. zm) oraz Kodeksu cywilnego.

XVI. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA

1. Wykonawcom, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy Prawo zamówień publicznych przysługują środki ochrony prawnej zgodnie z Działem VI ustawy Pzp.
2. Odwołanie przysługuje wyłącznie od niezgodnej z przepisami ustawy czynności zamawiającego podjętej w postępowaniu o udzielenie zamówienia lub zaniechania czynności, do której zamawiający jest zobowiązany na podstawie ustawy Pzp.
3. Odwołanie przysługuje wyłącznie wobec czynności:
   -opisu sposobu dokonywania oceny spełniania warunków udziału w postępowaniu
   -wykluczenia odwołującego z postępowania o udzielenie zamówienia
   -odrzucenia oferty odwołującego.

Załączniki:
1. Formularz ofertowy
2. Formularz oświadczeń wykonawcy
3. Szczegółowy opis parametrów technicznych

4. Wykaz osób biorących udział w realizacji zamówienia
5. Formularz cenowy – wyszczególnienie asortymentowe i ilościowe
6. Lista podmiotów należących do tej samej grupy kapitałowej
7. Wzór umowy

09. MAJ. 2014

DYREKTOR
Dariusz Jorg

KIEROWNIK
DZIAŁU ZAMÓWIEŃ PUBLICZNYCH
mgr Andrzej Rechowicz

D/ZP/381/44B/14
Załącznik nr 1

.....
pieczęć firmowa wykonawcy

OFERTA
DLA SAMODZIELNEGO PUBLICZNEGO SZPITALA KLINICZNEGO NR 5
ŚLĄSKIEGO UNIWERSYTETU MEDYCZNEGO W KATOWICACH

Nazwa wykonawcy .....

Siedziba: .....

REGON ..... NIP .....

Tel. ..... fax .....

Internet ..... e-mail .....

Ubiegając się o zamówienie publiczne na dostawę oprogramowania antywirusowego dla Uniwersyteckiego Centrum Okulistyki i Onkologii oferujemy realizację przedmiotowego zamówienia

za cenę netto ..... zł
podatek VAT .....% tj. ..... zł
Cena ofertowa z podatkiem VAT: .....zł
(słownie:.....zł)

Termin realizacji: Wykonawca w terminie 10 dni od daty podpisania umowy udzieli Zamawiającemu licencji i wdroży oprogramowanie na 234 stacjach roboczych w siedzibie Zamawiającego oraz przeszkoli administratora Zamawiającego.

Termin płatności: Zapłata za całość zamówienia nastąpi przelewem na wskazany na fakturze VAT rachunek Wykonawcy w terminie 30 dni od dnia otrzymania przez Zamawiającego prawidłowej i wystawionej zgodnie z umową faktury VAT.

- Zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia, nie wnosimy do niej zastrzeżeń oraz zdobyliśmy konieczne informacje do przygotowania oferty i zobowiązujemy się spełnić wszystkie wymienione w Specyfikacji wymagania Zamawiającego
- Jesteśmy związani niniejszą ofertą przez czas wskazany w Specyfikacji Istotnych Warunków Zamówienia tj. 30 dni od daty zakończenia terminu składania ofert.
- Zawarta w Specyfikacji Istotnych Warunków Zamówienia treść wzoru umowy została przez nas zaakceptowana i zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia umowy na wyżej wymienionych warunkach w miejscu i terminie wyznaczonym przez Zamawiającego
- Oświadczamy iż posiadamy prawo do dysponowania ww. oprogramowaniem w zakresie: sprzedaży, kopiowania, sprzedaży licencji .
- Znając treść art. 297 §1 Kodeksu Karnego *„Kto, w celu uzyskania dla siebie lub kogo innego, od banku lub jednostki organizacyjnej prowadzącej podobną działalność gospodarczą na podstawie ustawy albo od organu lub instytucji dysponujących środkami publicznymi - kredytu, pożyczki pieniężnej, poręczenia, gwarancji, akredytywy, dotacji, subwencji, potwierdzenia przez bank zobowiązania wynikającego z poręczenia lub gwarancji lub podobnego świadczenia pieniężnego na określony cel gospodarczy, elektronicznego instrumentu płatniczego lub zamówienia publicznego, przedkłada podrobiony, przerobiony, poświadczający nieprawdę albo nierzetelny dokument albo nierzetelne, pisemne oświadczenie dotyczące okoliczności o istotnym znaczeniu dla uzyskania wymienionego wsparcia finansowego, instrumentu płatniczego lub zamówienia podlega karze pozbawienia wolności od 3 miesięcy do lat 5"* , oświadczamy, że dane zawarte w ofercie, dokumentach i oświadczeniach są zgodne ze stanem faktycznym.

- Załącznikami do niniejszej oferty są *(wymienić wszystkie załączniki)* :

nazwa i numer dokumentu	**nr strony w ofercie**
.....	
.....	
.....	

.....
podpis i pieczęć osoby uprawnionej/osób uprawnionych
do reprezentowania wykonawcy

Emil Rybel

D/ZP/381/44B/14
Załącznik nr 2

.....
(nazwa i adres wykonawcy)

OŚWIADCZENIE

Dotyczy: postępowania o udzielenie zamówienia publicznego D/ZP/381/44B/14

Ja, niżej podpisany oświadczam, że wykonawca spełnia warunki, dotyczące:

1) posiadania uprawnień do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania;
2) posiadania wiedzy i doświadczenia;
3) dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia;
4) sytuacji ekonomicznej i finansowej.

.....
podpis i pieczęć osoby uprawnionej/osób
uprawnionych do reprezentowania wykonawcy

D/ZP/381/44B/14

.....
(nazwa i adres wykonawcy)

O Ś W I A D C Z E N I E

Dotyczy: postępowania o udzielenie zamówienia publicznego D/ZP/381/44B/14

Ja, niżej podpisany oświadczam, że wykonawca nie podlega wykluczeniu z postępowania w okolicznościach, o których mowa w art. 24 ust. 1 ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (Dz. U. z 2013 r. poz. 907, z późn. zm.).

.....
podpis i pieczęć osoby uprawnionej/ osób uprawnionych do reprezentowania wykonawcy

DN/ZP/381/44B/14
Załącznik nr 3

.....
pieczęć firmowa wykonawcy

SZCZEGÓŁOWY OPIS WYMAGAŃ I PARAMETRÓW TECHNICZNYCH

oprogramowania antywirusowego na stacje robocze wraz z konsolą do centralnej administracji:

Zamawiający obecnie posiada:

- 228 licencji pakietu antywirusowego ESET Smart Security Client na okres od 29.05.2012 do 28.05.2014 wraz z wdrożoną konsolą do centralnego zarządzania,
- 6 licencji pakietu antywirusowego ESET Smart Security Client na okres od 12.09.2013 do 15.09.2014 wraz z wdrożoną konsolą do centralnego zarządzania,
- 74 licencji pakietu antywirusowego ESET Smart Security Client na okres od 09.07.2013 do 13.07.2015 wraz z wdrożoną konsolą do centralnego zarządzania,
- 7 licencji pakietu antywirusowego ESET Smart Security Client na okres od 12.09.2013 do 16.09.2015 wraz z wdrożoną konsolą do centralnego zarządzania.

W ramach zamówienia Zamawiający wymaga dostarczenia aktualizacji 234 licencji do posiadanego oprogramowania antywirusowego lub dostarczenia nowego równoważnego rozwiązania.

W przypadku dostarczenia nowego równoważnego rozwiązania Zamawiający wymaga wdrożenia i uruchomienia konsoli centralnego zarządzania oraz konfiguracji wszystkich stacji roboczych wraz z deinstalacją obecnie używanego oprogramowania.

Lp.	***Wymagania minimalne***	***Czy spełnia? (tak/nie)***
1	Pakiet musi posiadać:	----------
A	wersja oprogramowania - polskojęzyczna w całości	
B	licencja na okres 12 miesięcy od dnia 29.05.2014	
C	licencja zbiorcza na zamawianą ilość stanowisk (jeden klucz) dla posiadanych aktualnie 228 licencji (29.05.2012 do 28.05.2014) oraz 6 licencji (12.09.2013 do 15.09.2014) = łącznie 234 licencje na jednym kluczu	
D	konsola centralnego zarządzania	
2	Oferowany pakiet bezpieczeństwa:	----------
Wymagania dla rozwiązania równoważnego (podać nazwę i wersję oferowanego rozwiązania poniżej):		----------
.....		
Wymagania licencyjne:		----------
A	licencje na oprogramowanie antywirusowe wraz z pakietem bezpieczeństwa dla 234 stacji roboczych	
B	konsola wraz z wdrożeniem do centralnego zarządzania oprogramowaniem (w przypadku zaoferowania oprogramowania innego niż posiadane dotychczas przez Zamawiającego) z możliwością instalacji na dowolnej liczbie stanowisk i dowolnej liczby serwerów do zdalnej administracji	
Wymagania dla pakietu antywirusowego wraz z pakietem bezpieczeństwa:		
C	*Wymagania ogólne dla stacji roboczych:* • Pełne wsparcie dla systemu Windows 2000/XP/Vista/Windows 7/Windows 8 • Wsparcie dla Windows Security Center (Windows XP SP2)	

Paweł Rytel

	• Wsparcie dla 32- i 64-bitowej wersji systemu Windows • Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim • Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim • Skuteczność programu potwierdzona nagrodami VB100 i co najmniej dwie inne niezależne organizacje takie jak ICSA labs lub Check Mark • Wydajność wg testów przeprowadzonego przez niezależną organizacją AntiVirus-Comparative i zaklasyfikowany: - w teście Real-World protection Test na poziomie Advanced+ (XII 2013) - w teście Anti-Phishing Test na poziomie Advanced+ (VIII 2013) - w teście Heuristic Behavioural Test na poziomie Advanced+ (III 2013) - w teście Removal Test na poziomie Advanced+ (XI 2013) - w teście Retrospective Test na poziomie Advanced+ (XI 2013) - w pozostałych testach przynajmniej na poziomie Advanced	
D	*Ochrona antywirusowa i antyspyware:* • Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. • Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. • Wbudowana technologia do ochrony przed rootkitami. • Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. • Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. • System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania. • Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). • Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. • Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu. • Możliwość skanowania dysków sieciowych i dysków przenośnych. • Skanowanie plików spakowanych i skompresowanych. • Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń). • Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. • Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. • Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. • Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas, co najmniej 10 min lub do ponownego uruchomienia komputera.	

	• W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. • Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. • Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. • Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird do wersji 5.x i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego). • Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird do wersji 5.x i Windows Live Mail. • Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). • Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. • Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie. • Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. • Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. • Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony. • Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora. • Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. • Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie. • Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. • Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. • Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego. • Aplikacja musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. • Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.	

	• Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. • W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne. • Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie. • Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. • Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika. • Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. • Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. • Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. • Interfejs programu ma oferować funkcję pracy w trybie bez grafiki gdzie cały interfejs wyświetlany jest w formie formatek i tekstu. • Interfejs programu ma mieć możliwość automatycznego aktywowania trybu bez grafiki w momencie, gdy użytkownik przełączy system Windows w tryb wysokiego kontrastu. • Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła. • Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło. • Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji musi być takie samo. • Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji. • Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. • Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.	

Szuf Rypta

	• System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. • System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. • Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: stacji dyskietek, napędów CD/DVD, czytników kart, urządzeń Bluetooth, portów LPT/COM. • Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model. • Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia. • Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. • W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. • Użytkownik ma posiadać możliwość takiej konfiguracji aplikacji aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika • Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). • Moduł HIPS musi posiadać możliwość pracy w jednym z czterech trybów: o tryb automatyczny z regułami gdzie aplikacja automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, o tryb interaktywny, w którym to aplikacja pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, o tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, o tryb uczenia się, w którym aplikacja uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu aplikacja musi samoczynnie przełączyć się w tryb pracy oparty na regułach. • Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. • Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. • Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach. • Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. • Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu,	

Bil Kytel

	jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. • Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. • Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami. • Aplikacja musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. • Aplikacja musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http • Aplikacja musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback). • Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa). • Aplikacja musi być w pełni zgodna z technologią Network Access Protection (NAP). • Program ma być w pełni zgodny z technologią CISCO Network Access Control. • Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym. • W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji. • Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie aplikacja włączała powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie. • Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania. • Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. • W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór następujących modułów do instalacji: ochrona antywirusowa i antyspywerowa, kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, kopia dystrybucyjna, Obsługa technologii Microsoft NAP.	
E	*Ochrona przed spamem:* • Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail, Windows Live Mail oraz Mozilla Thunderbird do wersji 5.x wykorzystująca filtry Bayes-a, białą i czarną listę oraz bazę charakterystyk wiadomości spamowych. • Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. • Pełna integracja z programami pocztowymi MS Outlook, Outlook Express, Windows Mail, Windows Live Mail oraz Mozilla Thunderbird do wersji 5.x – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu	

	programu pocztowego. • Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. • Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym. • Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam. • Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam. • Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci" obecnym w programie Microsoft Outlook. • Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana" oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana". • Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.	
F	*Zapora osobista (personal firewall):* • Zapora osobista ma pracować jednym z 5 trybów: ○ tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, ○ tryb automatyczny z wyjątkami - działa podobnie jak tryb automatyczny, ale umożliwia administratorowi zdefiniowanie wyjątków dla ruchu przychodzącego i wychodzącego w liście reguł, ○ tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo), ○ tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany, ○ tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji. • Możliwość tworzenia list sieci zaufanych. • Możliwość dezaktywacji funkcji zapory sieciowej na kilka sposobów: pełna dezaktywacja wszystkich funkcji analizy ruchu sieciowego, tylko skanowanie chronionych protokołów oraz dezaktywacja do czasu ponownego uruchomienia komputera. • Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego. • Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję. • Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń. • Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu. • Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet. • Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.	

	• Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu. • Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. • Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci. • Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci • Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora. • Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, aktywności wyłącznie jednego połączenia sieciowego lub wielu połączeń sieciowych konkretny interfejs sieciowy w systemie. • Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS zarówno z wykorzystaniem adresów IPv4 jak i IPv6 • Opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem zwiększenia dokładności identyfikacji danej sieci. • Możliwość aktualizacji sterowników zapory osobistej po restarcie komputera.	
G	*Kontrola dostępu do stron internetowych:* • Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych. • Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły. • Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego. • Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika. • Aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 140 kategorii i pod kategorii. • Podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii. • Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta. • Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.	
H	*Konsola zdalnej administracji:* • Centralna instalacja programów służących do ochrony stacji roboczych Windows. • Centralne zarządzanie programami służącymi do ochrony stacji roboczych Windows/ Linux/ MAC OS.	

	• Centralna instalacja oprogramowania na końcówkach (stacjach roboczych) z systemami operacyjnymi typu 2000/XP Professional/Vista/Windows7. • Do instalacji centralnej i zarządzania centralnego nie jest wymagany dodatkowy agent. Na końcówkach zainstalowany jest sam program antywirusowy • Komunikacja miedzy serwerem a klientami może być zabezpieczona hasłem. • Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci. • Kreator konfiguracji zapory osobistej stacji klienckich pracujących w sieci, umożliwiający podgląd i utworzenie globalnych reguł w oparciu o reguły odczytane ze wszystkich lub z wybranych komputerów lub ich grup. • Możliwość uruchomienia centralnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej. • Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych). • Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacja robocza należy. • Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu. • Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych. • Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów. • Możliwość importowania konfiguracji programu z wybranej stacji roboczej a następnie przesłanie (skopiowanie) jej na inną stację lub grupę stacji roboczych w sieci. • Możliwość zmiany konfiguracji na stacjach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko, jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne). • Możliwość uruchomienia serwera centralnej administracji i konsoli zarządzającej na stacjach Windows 2000/XP/Vista/Windows 7 oraz na serwerach 2000/2003/2008/2008R2 – 32 i 64-bitowe systemy. • Możliwość rozdzielenia serwera centralnej administracji od konsoli zarządzającej, w taki sposób, że serwer centralnej administracji jest instalowany na jednym serwerze/ stacji a konsola zarządzająca na tym samym serwerze i na stacjach roboczych należących do administratorów. • Możliwość wymuszenia konieczności uwierzytelniania stacji roboczych przed połączeniem się z serwerem zarządzającym. Uwierzytelnianie przy pomocy zdefiniowanego na serwerze hasła. • Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie żadnych dodatkowych baz typu MSDE lub MS SQL. Serwer centralnej administracji musi mieć własną wbudowaną bazę w pełni kompatybilną z formatem bazy danych programu Microsoft Access. • Serwer centralnej administracji ma oferować administratorowi możliwość współpracy przynajmniej z	

	trzema zewnętrznymi motorami baz danych w tym minimum z: Microsoft SQL Server, MySQL Server oraz Oracle. • Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie dodatkowych aplikacji takich jak Internet Information Service (IIS) czy Apache. • Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) w formacie HTML lub CSV. • Aplikacja musi posiadać funkcjonalność, która umożliwi przesłanie wygenerowanych raportów na wskazany adres email. • Do wysłania raportów aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na stacji gdzie jest uruchomiona usługa serwera. • Możliwość tworzenia hierarchicznej struktury serwerów zarządzających i replikowania informacji pomiędzy nimi w taki sposób, aby nadrzędny serwer miał wgląd w swoje stacje robocze i we wszystkie stacje robocze serwerów podrzędnych (struktura drzewiasta). • Serwer centralnej administracji ma oferować funkcjonalność synchronizacji grup komputerów z drzewem Active Directory. Po synchronizacji automatycznie są umieszczane komputery należące do zadanych grup w AD do odpowiadających im grup w programie. Funkcjonalność ta nie może wymagać instalacji serwera centralnej administracji na komputerze pełniącym funkcję kontrolera domeny. • Serwer centralnej administracji ma umożliwiać definiowanie różnych kryteriów wobec podłączonych do niego klientów (w tym minimum przynależność do grupy roboczej, przynależność do domeny, adres IP, adres sieci/podsieci, zakres adresów IP, nazwa hosta, przynależność do grupy, brak przynależności do grupy). Po spełnieniu zadanego kryterium lub kilku z nich stacja ma otrzymać odpowiednią konfigurację. • Serwer centralnej administracji ma być wyposażony w mechanizm informowania administratora o wykryciu nieprawidłowości w funkcjonowaniu oprogramowania zainstalowanego na klientach w tym przynajmniej informowaniu o: wygaśnięciu licencji na oprogramowanie, o tym że zdefiniowany procent z pośród wszystkich stacji podłączonych do serwera ma nieaktywną ochronę, oraz że niektórzy z klientów podłączonych do serwera oczekują na ponowne uruchomienie po aktualizacji do nowej wersji oprogramowania. • Serwer centralnej administracji ma być wyposażony w wygodny mechanizm zarządzania licencjami, który umożliwi sumowanie liczby licencji nabytych przez użytkownika. Dodatkowo serwer ma informować o tym, ilu stanowiskową licencję posiada użytkownik i stale nadzorować ile licencji spośród puli nie zostało jeszcze wykorzystanych. • W sytuacji, gdy użytkownik wykorzysta wszystkie licencje, które posiada po zakupie oprogramowania, administrator po zalogowaniu się do serwera poprzez konsolę administracyjną musi zostać poinformowany o tym fakcie za pomocą okna informacyjnego. • Możliwość tworzenia repozytorium aktualizacji na serwerze centralnego zarządzania i udostępniania go przez wbudowany serwer http. • Aplikacja musi posiadać funkcjonalność, która umożliwi dystrybucję aktualizacji za pośrednictwem szyfrowanej komunikacji (za pomocą protokołu https). • Do celu aktualizacji za pośrednictwem protokołu https nie jest wymagane instalowanie dodatkowych zewnętrznych	

	usług jak IIS lub Apache zarówno od strony serwera aktualizacji jak i klienta. • Dostęp do kwarantanny klienta ma być z poziomu systemu centralnego zarządzania. • Możliwość przywrócenia lub pobrania zainfekowanego pliku ze stacji klienckiej przy wykorzystaniu centralnej administracji. • Administrator ma mieć możliwość przywrócenia i wyłączenia ze skanowania pliku pobranego z kwarantanny stacji klienckiej. • Podczas przywracania pliku, administrator ma mieć możliwość zdefiniowania kryteriów dla plików, które zostaną przywrócone w tym minimum: zakres czasu z dokładnością co do minuty kiedy wykryto daną infekcję, nazwa danego zagrożenia, dokładna nazwa wykrytego obiektu oraz zakres minimalnej i maksymalnej wielkości pliku z dokładnością do jednego bajta. • Możliwość utworzenia grup, do których przynależność jest aplikowana dynamicznie na podstawie zmieniających się parametrów klientów w tym minimum w oparciu o: wersję bazy sygnatur wirusów, maskę wersji bazy sygnatur wirusów, nazwę zainstalowanej aplikacji, dokładną wersję zainstalowanej aplikacji, przynależność do domeny lub grupy roboczej, przynależność do serwera centralnego zarządzania, przynależności lub jej braku do grup statycznych, nazwę komputera lub jej maskę, adres IP, zakres adresów IP, przypisaną politykę, czas ostatniego połączenia z systemem centralnej administracji, oczekiwania na restart, ostatnie zdarzenie związane z wirusem, ostatnie zdarzenie związane z usługą programu lub jego procesem, ostatnie zdarzenie związane ze skanowaniem na żądanie oraz z nieudanym leczeniem podczas takiego skanowania, maską wersji systemu operacyjnego oraz flagą klienta mobilnego. • Podczas tworzenia grup dynamicznych, parametry dla klientów można dowolnie łączyć oraz dokonywać wykluczeń pomiędzy nimi. • Utworzone grupy dynamiczne mogą współpracować z grupami statycznymi. • Możliwość definiowania administratorów o określonych prawach do zarządzania serwerem administracji centralnej (w tym możliwość utworzenia administratora z pełnymi uprawnieniami lub uprawnienia tylko do odczytu). • W przypadku tworzenia administratora z niestandardowymi uprawnieniami możliwość wyboru modułów, do których ma mieć uprawnienia: zarządzanie grupami, powiadomieniami, politykami, licencjami oraz usuwanie i modyfikacja klientów, zdalna instalacja, generowanie raportów, usuwanie logów, zmiana konfiguracji klientów, aktualizacja zdalna, zdalne skanowanie klientów, zarządzanie kwarantanna na klientach. • Możliwość synchronizowania użytkowników z Active Directory w celu nadania uprawnień administracyjnych do serwera centralnego zarządzania. • Wszystkie działania administratorów zalogowanych do serwera administracji centralnej mają być logowane. • Możliwość uruchomienia panelu kontrolnego dostępnego za pomocą przeglądarki internetowej. • Panel kontrolny musi umożliwiać administratorowi wybór elementów monitorujących, które mają być widoczne. • Administrator musi posiadać możliwość tworzenia wielu zakładek, w których będą widoczne wybrane przez administratora elementy monitorujące. • Elementy monitorujące muszą umożliwiać podgląd w postaci graficznej co najmniej: bieżącego obciążenia serwera	

Daniel Rytel

	zarządzającego, statusu serwera zarządzającego, obciążenia bazy danych z której korzysta serwer zarządzający, obciążenia komputera, na którym zainstalowana jest usługa serwera zarządzającego, informacji odnośnie komputerów z zainstalowaną aplikacja antywirusową, a które nie są centralnie zarządzane, podsumowania modułu antyspamowego, informacji o klientach znajdujących się w poszczególnych grupach, informacji o klientach z największą ilością zablokowanych stron internetowych, klientach, na których zostały zablokowane urządzenia zewnętrzne, informacje na temat greylistingu, podsumowania wykorzystywanych systemach operacyjnych, informacje odnośnie spamu sms, zagrożeń oraz ataków sieciowych • Administrator musi posiadać możliwość maksymalizacji wybranego elementu monitorującego. • Możliwość włączenia opcji pobierania aktualizacji z serwerów producenta z opóźnieniem. • Możliwość przywrócenia baz sygnatur wirusów wstecz (tzw. Rollback). • Aplikacja musi mieć możliwość przygotowania paczki instalacyjnej dla stacji klienckiej, która będzie pozbawiona wybranej funkcjonalności. • Wsparcie dla protokołu IPv6 • Administrator musi posiadać możliwość centralnego, tymczasowego wyłączenia wybranego modułu ochrony na stacji roboczej. • Centralne tymczasowe wyłączenie danego modułu nie może skutkować koniecznością restartu stacji roboczej. • Aplikacja musi posiadać możliwość natychmiastowego uruchomienia zadania znajdującego się w harmonogramie bez konieczności oczekiwania do jego zaplanowanego czasu. • Aplikacja do administracji centralnej musi umożliwiać utworzenie nośnika, za pomocą którego będzie istniała możliwość przeskanowania dowolnego komputera objętego licencją przed startem systemu. • Administrator musi posiadać możliwość określenia ilości jednoczesnych wątków instalacji centralnej oprogramowania klienckiego.	

.....
podpis i pieczęć osoby uprawnionej/ osób uprawnionych do reprezentowania wykonawcy

DN/ZP/381/44B/14
Załącznik nr 3

.....
pieczęć firmowa wykonawcy

WYKAZ OSÓB
KTÓRE BĘDĄ UCZESTNICZYĆ W WYKONANIU NINIEJSZEGO ZAMÓWIENIA

OŚWIADCZAM(Y), ŻE:

Zamówienie niniejsze wykonywać będą następujące osoby:

L.p.	**Imię i Nazwisko**	**Zakres wykonywanych czynności**
1		
2		
3		

Należy dołączyć certyfikaty wydane dla w/w osób przez producenta oprogramowania lub dystrybutora

.....
podpis i pieczęć osoby uprawnionej/osób uprawnionych
do reprezentowania wykonawcy

DN/ZP/3800/54B/12
Załącznik nr 4

.....
pieczęć firmowa wykonawcy

W zależności od oferowanego oprogramowania wypełnić odpowiednio tabelę nr 1 lub tabelę nr 2

Formularz cenowy
wyszczególnienie asortymentowe i ilościowe

(Zamawiający posiada oprogramowanie antywirusowe ESET Smart Security Business Edition Client - 228 licencji na oprogramowanie antywirusowe dla stacji roboczych łącznie z firewallem - termin ważności licencji wskazano w załączniku nr 3 do SIWZ)

Tabela nr 1 (dla Wykonawcy dostarczającego oprogramowanie ESET)

Przedmiot zamówienia	**NAZWA/ PRODUCENT**	**CENA** Jednostkowa netto	**Wartość netto**	**Podatek VAT %**	**WARTOŚĆ BRUTTO**
234 licencje przedłużających na oprogramowanie antywirusowe dla stacji roboczych łącznie z firewallem	ESET Smart Security Business Edition Client				
RAZEM					

Tabela nr 2 (dla Wykonawcy dostarczającego oprogramowanie równoważne)

Przedmiot zamówienia	**NAZWA/ PRODUCENT**	**CENA** Jednostkowa netto	**Wartość netto**	**Podatek VAT %**	**WARTOŚĆ BRUTTO**
234 licencje na oprogramowanie antywirusowe dla stacji roboczych łącznie z firewallem oraz konsolą do centralnego zarządzania i wdrożeniem całości					
	RAZEM				

.....
podpis i pieczęć osoby uprawnionej/osób uprawnionych
do reprezentowania wykonawcy

D/ZP/381/44B/14
Załącznik nr 6

.....
pieczęć firmowa wykonawcy

LISTA PODMIOTÓW NALEŻĄCYCH DO TEJ SAMEJ GRUPY KAPITAŁOWEJ CO WYKONAWCA

w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. Nr 50, poz. 331, z późn. zm.)*

1. .....
2. .....
3. .....
4. .....

.....
podpis i pieczęć osoby uprawnionej/osób uprawnionych do reprezentowania wykonawcy

Oświadczam, że wykonawca składający ofertę nie należy do grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. Nr 50, poz. 331, z późn. zm.)*

.....
podpis i pieczęć osoby uprawnionej/osób uprawnionych do reprezentowania wykonawcy

*niepotrzebne skreślić

D/ZP/381/44B/14
Załącznik nr 1

UMOWA – wzór

zawarta w dniu ..... w Katowicach.

Strony umowy:
Zamawiający – Uniwersyteckie Centrum Okulistyki i Onkologii Samodzielny Publiczny Szpital Kliniczny Śląskiego Uniwersytetu Medycznego w Katowicach, 40-514 Katowice, ul. Ceglana 35
KRS 0000049660, NIP 954-22-74-017, REGON 001325767
reprezentowane przez:
Dariusza Jorg – Dyrektora
Wykonawca – .....
KRS ....., REGON ....., NIP .....
reprezentowany przez:

.....

.....

W wyniku przeprowadzenia przez Zamawiającego postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego – zgodnie z ustawą z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz.U.2013.907 j.t. z późn. zm.) (dalej zwanej: „PZP") została zawarta umowa następującej treści:

§ 1.
PRZEDMIOT UMOWY

1. Na podstawie oferty wybranej w postępowaniu Zamawiający zamawia, a Wykonawca przyjmuje do wykonania na zasadach określonych w Specyfikacji Istotnych Warunków Zamówienia: udzielenie licencji oraz wdrożenie oprogramowania antywirusowego wyszczególnionego w załączniku nr 1 do umowy, a także przeszkolenie administratora Zamawiającego z zakresu obsługi oprogramowania.
2. Wdrożenie oprogramowania antywirusowego polegać będzie na jego zainstalowaniu na stacjach roboczych wskazanych przez Zamawiającego oraz skonfigurowaniu konsoli do zdalnego zarządzania oprogramowaniem.

§ 2.
WARUNKI REALIZACJI UMOWY

1. Wykonawca w terminie 10 dni od daty podpisania umowy udzieli Zamawiającemu licencji i wdroży oprogramowanie na 234 stacjach roboczych w siedzibie Zamawiającego.
2. W terminie określonym w ust. 1 Wykonawca dostarczy dokumentację użytkową (instrukcję obsługi) w języku polskim, opisującą podstawowe funkcje dostarczonego oprogramowania. W przypadku zmiany w zakresie obsługi lub zmiany funkcji oprogramowania Wykonawca niezwłocznie poinformuje o tym Zamawiającego dostarczając jednocześnie Zamawiającemu aktualną dokumentację użytkową.
3. Wykonawca jest zobowiązany do przeprowadzenia wdrożenia oprogramowania antywirusowego opisanego w załączniku nr 1 do umowy oraz przeszkolenia administratora z zakresu obsługi oprogramowania. Wdrożenie oraz szkolenie przeprowadzone musi być przez pracownika Wykonawcy posiadającego certyfikat wydany przez producenta oprogramowania lub dystrybutora. Wdrożenie oprogramowania i przeszkolenie administratora nastąpi w ciągu 10 dni kalendarzowych od dnia podpisania umowy.
4. Wykonawca zapewnia administratorowi Zamawiającego wsparcie telefoniczne dotyczące konfiguracji oraz rozwiązywania problemów z oprogramowaniem dla stacji roboczych i serwerów w okresie 24 miesięcy od daty .....
5. Potwierdzeniem odbioru licencji, wdrożenia oprogramowania, dostarczenia dokumentacji użytkowej i przeszkolenia administratora będzie protokół podpisany przez przedstawicieli Zamawiającego i Wykonawcy.

§ 3
GWARANCJE

1. Wykonawca udziela na dostarczone oprogramowanie 12-miesięcznego wsparcia serwisowego rozpoczynającego swój bieg od daty wdrożenia oprogramowania.
2. Zamawiający może zgłaszać Wykonawcy nieprawidłowe działanie zakupionego oprogramowania

2. Zamawiający może zgłaszać Wykonawcy nieprawidłowe działanie zakupionego oprogramowania (awarie) w godzinach swojej pracy (od godz. ..... do godz. .....) od poniedziałku do piątku. Zgłoszenia wad, usterek, awarii i zaleceń serwisowych będą przesyłane za pomocą faksu, poczty elektronicznej lub telefonicznie. Zgłoszenie telefoniczne musi być potwierdzone faksem lub e-mailem.
3. W przypadku awarii Wykonawca zapewnia odpowiednie wsparcie (telefon, mail lub fax) w terminie ..... od chwili zgłoszenia awarii.

§ 4
WYNAGRODZENIE I WARUNKI PŁATNOŚCI

1. Łączna cena za zrealizowanie całego przedmiotu umowy określonego w § 1 wynosi netto .....złotych plus należny podatek VAT ....% tj.....złotych. Razem: .....złotych (słownie: .....)
2. Cena określona w ust. 1 obejmuje wszystkie koszty związane z realizacją przedmiotu umowy, a w szczególności: koszty konfiguracji, koszty przejazdów i pobytów serwisanta u Zamawiającego, koszt opakowania, dostarczenia, ubezpieczenia oprogramowania, koszt instalacji, cła i podatki, koszt wsparcia telefonicznego, koszt nośników na których zostało dostarczone oprogramowanie.
3. Zapłata za wykonanie zamówienia nastąpi przelewem na wskazany na fakturze VAT rachunek Wykonawcy, w terminie 30 dni od dnia otrzymania przez Zamawiającego prawidłowej i wystawionej zgodnie z umową faktury VAT. W przypadku gdyby Wykonawca zamieścił na fakturze inny termin płatności niż określony w niniejszej umowie, obowiązuje termin płatności określony w umowie.
4. Faktura, o której mowa w ust. 3 powyżej nie może zostać wystawiona wcześniej niż data podpisania przez obie strony protokołu, o którym mowa w § 2 ust. 5 umowy.
5. Za datę zapłaty przyjmuje się datę obciążenia rachunku bankowego Zamawiającego.

§ 5
KARY UMOWNE

1. Wykonawca zapłaci Zamawiającemu kary umowne:
   a) w wysokości 0,2 % wartości brutto przedmiotu umowy określonego w § 4 ust. 1 za każdy dzień opóźnienia w realizacji któregokolwiek z obowiązków określonych w § 2 ust. 1, ust. 2 i ust. 3 umowy
   b) w wysokości 10% wartości brutto przedmiotu umowy określonego w § 4 ust. 1 niniejszej umowy – w przypadku odstąpienia lub rozwiązania umowy ze skutkiem natychmiastowym z przyczyn, za które odpowiada Wykonawca.
2. Zamawiający ma prawo dochodzić kar umownych poprzez potrącenie ich na podstawie księgowej noty obciążeniowej z jakimikolwiek należnościami Wykonawcy. W przypadku braku możliwości zaspokojenia roszczeń z tytułu kar umownych na zasadach określonych powyżej, nota księgowa obciążeniowa płatna będzie do 14 dni od daty jej otrzymania przez Wykonawcę.
3. W przypadku, gdy wysokość wyrządzonej szkody przewyższa naliczoną karę umowną Zamawiający ma prawo żądać odszkodowania uzupełniającego na zasadach ogólnych.

§ 6.
ROZWIĄZANIE I ODSTĄPIENIE OD UMOWY

1. W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, Zamawiający może odstąpić od umowy w terminie 30 dni od daty powzięcia wiadomości o takich okolicznościach. W takim wypadku Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy.
2. Zamawiający może rozwiązać umowę ze skutkiem natychmiastowym w przypadku, gdy:
   a) opóźnienie w zrealizowaniu dostawy przekroczy 10 dni kalendarzowych;
   b) Wykonawca opóźni się z realizacją obowiązków określonych w § 2 ust. 3 umowy o ponad 14 dni kalendarzowych.
3. Oświadczenie Zamawiającego o rozwiązaniu umowy zostanie wysłane listem poleconym na adres Wykonawcy podany w umowie.
4. Rozwiązanie umowy na podstawie ust. 2 niniejszego paragrafu nie zwalnia Wykonawcy od obowiązku zapłaty kar umownych i odszkodowań.

§ 7.
POSTANOWIENIA KOŃCOWE

1. Umowa zawarta jest na okres od ..... do .....
2. W sprawach nieuregulowanych niniejszą umową mają zastosowanie odpowiednie przepisy ustawy -

Prawo zamówień publicznych i Kodeksu Cywilnego.

3. W przypadku niejasności w zapisach niniejszej umowy Strony mogą odwołać się do zapisów w Specyfikacji Istotnych Warunków Zamówienia.
4. Wykonawca nie może bez uzyskania wcześniejszej pisemnej zgody Zamawiającego, przelać jakichkolwiek praw lub obowiązków wynikających z niniejszej umowy na osoby trzecie. Czynność prawna mająca na celu zmianę wierzyciela może nastąpić wyłącznie po uprzednim wyrażeniu pisemnej zgody przez podmiot tworzący Zamawiającego.
5. Wszelkie spory wynikłe na tle realizacji umowy będzie rozstrzygał sąd powszechny właściwy dla siedziby Zamawiającego.
6. Zakazuje się istotnych zmian postanowień zawartej umowy w stosunku do treści wybranej oferty za wyjątkiem zmian przewidzianych przez Zamawiającego i na określonych przez niego warunkach.
7. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, dwa egzemplarze dla Zamawiającego, jeden egzemplarz dla Wykonawcy.

Załączniki do umowy:
1.Formularz asortymentowo-cenowy

Wykonawca

Zamawiający

Z-CA GŁÓWNEGO KSIEGOWEGO
Beata Paszkowska

RADCA PRAWNY
Joanna Kempart

D/ZP/381/44B/14
Załącznik nr 6

.....
pieczęć firmowa wykonawcy

W zależności od oferowanego oprogramowania wypełnić odpowiednio tabelę nr 1 lub tabelę nr 2

Formularz cenowy
wyszczególnienie asortymentowe i ilościowe

(Zamawiający posiada oprogramowanie antywirusowe ESET Smart Security Client - 234 licencje na oprogramowanie antywirusowe dla stacji roboczych łącznie z firewallem)

Tabela nr 1

Przedmiot zamówienia	**NAZWA/ PRODUCENT**	**CENA** Jednostkowa netto	**Wartość netto**	**Podatek VAT %**	**WARTOŚĆ BRUTTO**
228 licencji przedłużających na oprogramowanie antywirusowe dla stacji roboczych łącznie z firewallem	ESET Smart Security Client				
RAZEM					

Tabela nr 2

Przedmiot zamówienia	**NAZWA/ PRODUCENT**	**CENA** Jednostkowa netto	**Wartość netto**	**Podatek VAT %**	**WARTOŚĆ BRUTTO**
228 licencji na oprogramowanie antywirusowe dla stacji roboczych łącznie z firewallem					
1 konsola do centralnego zarządzania niniejszym oprogramowaniem	*wliczone w cenę oprogramowania*				
wdrożenie konsoli	*wliczone w cenę oprogramowania*				
	RAZEM				

.....
podpis i pieczęć osoby uprawnionej/osób uprawnionych
do reprezentowania wykonawcy