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

Znak sprawy : D/ZP/381/63BB/15

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

Na dostawę licencji oprogramowania antywirusowego

Postępowanie o udzielenie zamówienia prowadzone jest w trybie **przetargu nieograniczonego poniżej 134 000 EURO** na podstawie ustawy z dnia 29 stycznia 2004 roku Prawo Zamówień Publicznych (tekst jednolity: Dz. U. z 2013 r. poz.907 z późn.zm)

Specyfikację istotnych warunków zamówienia
wraz z załącznikami

Zatwierdził w dniu 20.08.2015r.

Z upoważnienia D Y R E K T O R A
Uniwersyteckiego Centrum Okulistyki i Onkologii
w Katowicach

mgr inż. Renata Kantczak
Z-ca Dyrektora ds. Ekonomiczno-Gospodarczych

I. 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. 32/3581200 lub 32/358-13-32 fax. 32 251-84-37 lub 32/358-14-32
Internet : www.klinika.katowice.pl e-mail : zp@szpitalceglana.pl

II. TRYB UDZIELENIA ZAMÓWIENIA:

Postępowanie o udzielenie zamówienia prowadzone jest w trybie przetargu nieograniczonego na podstawie ustawy z dnia 29 stycznia 2004 roku Prawo Zamówień Publicznych (tekst jednolity: Dz. U. z 2013 r. poz.907 z późn.zm)

III. PRZEDMIOT ZAMÓWIENIA

1. Przedmiotem zamówienia jest dostawa licencji oprogramowania antywirusowego :
   - **330** licencji oprogramowania antywirusowego zabezpieczającego stacje robocze
   - **10** licencji oprogramowania antywirusowego zabezpieczającego urządzenia mobilne tj. laptopy (systemy Windows), tablety (system Android),
   - **3** licencji zabezpieczających serwery (System Linux, Windows Server)
2. Zamawiający obecnie posiada pakiet antywirusowy ESET Endpoint Security Client dla stacji roboczych (w sumie 315 licencji) wraz z wdrożoną konsolą do centralnego zarządzania. W przypadku zaoferowania takiego samego pakietu antywirusowego Zamawiający nie wymaga dostawy konsoli centralnego zarządzania oraz wdrożenia dostarczonego oprogramowania i przeszkolenia .
3. **(*)**Zamawiający dopuszcza możliwość zaoferowania oprogramowania równoważnego do wskazanego , który posiada pod warunkiem spełniania wymagań określonych w załaczniku nr 4 SIWZ , oraz dostawy konsoli centralnego zarządzania wraz z instalacją i konfiguracją , wdrożenia u Zamawiającego Oprogramowania, przeszkolenia w zakresie obsługi dostarczonego Oprogramowania trzech wskazanych przez Zamawiającego pracowników.
4. Nazwy i kody wg Wspólnego Słownika Zamówień:
   48.76.00.00-3 Pakiety oprogramowania do ochrony antywirusowej
   48.76.10.00-0 Pakiety oprogramowania antywirusowego
   48.00.00.00-8 – pakiety oprogramowania i systemy informatyczne
5. Przedmiot i warunki realizacji niniejszego zamówienia winny być zgodne z obowiązującymi przepisami prawnymi w tym zakresie.

IV. TERMIN WYKONANIA ZAMÓWIENIA:

Wykonawca w terminie 7 dni roboczych od daty zawarcia umowy udzieli Zamawiającemu licencji na Oprogramowanie, wdroży Oprogramowanie **(*)** oraz przeszkoli trzech wskazanych przez Zamawiającego pracowników z zakresu obsługi Oprogramowania **(*)**.
Licencja zostanie udzielona na okres dwóch lat od daty podpisania Protokołu Odbioru Oprogramowania

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
- sytuacji ekonomicznej i finansowej

Zamawiający nie stawia szczegółowych warunków - za spełniających te warunki Zamawiający uzna Wykonawców, którzy przedłożą oświadczenie o spełnianiu warunków udziału w postępowaniu stanowiące załącznik nr 2 do siwz

2. Ponadto o udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:
- nie podlegają wykluczeniu z postępowania o udzielenie zamówienia (art. 24 ust. 1 ustawy Pz
- 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, zdolnościach finansowych lub ekonomicznych innych podmiotów, niezależnie od charakteru prawnego łączących go z nimi stosunków. Wykonawca w takiej sytuacji zobowiązany jest udowodnić zamawiającemu, iż będzie dysponował tymi zasobami w trakcie realizacji zamówienia, w szczególności przedstawiając w tym celu pisemne zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby wykonania zamówienia.

4. Podmiot ,który zobowiązał się do udostępnienia zasobów zgodnie z art.26 ust.2b,będzie odpowiadał solidarnie z wykonawcą za szkodę zamawiającego powstałą wskutek nieudostępnienia tych zasobów chyba że za nieudostępnienie zasobów nie ponosi winy.
5. 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 stanowiące załącznik nr 2 do SIWZ.

2. **W celu wykazania braku podstaw do wykluczenia z postępowania o udzielenie zamówienia <u>w okolicznościach o których mowa w art. 24 ust.1 ustawy Wykonawca dołączy do oferty :</u>**

a) oświadczenie o braku podstaw do wykluczenia – załącznik nr 3 do SIWZ
b) aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji , 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.

Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej składa dokument wystawiony w kraju w którym ma siedzibę lub miejsce zamieszkania potwierdzający że nie otwarto jego likwidacji ani nie ogłoszono upadłości. Jeżeli w miejscu zamieszkania osoby lub w kraju w którym wykonawca ma siedzibę lub miejsce zamieszkania nie wydaje się dokumentu , zastępuje się je dokumentem zawierającym oświadczenie ,w którym określa się także osoby uprawnione do reprezentacji wykonawcy, złożone przed właściwym organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego odpowiednio kraju miejsca zamieszkania osoby lub kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, lub przed notariuszem.

3. **<u>W celu wykazania braku podstaw do wykluczenia z postępowania o udzielenie zamówienia w okolicznościach, o których mowa w art. 24 ust.2 pkt 5 ustawy</u>** Wykonawca dołączy do oferty listę podmiotów należących do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, o której mowa w art.24 ust.2 pkt.5 ustawy Prawo zamówień publicznych lub informację o tym, że nie należy do grupy kapitałowej – załącznik nr 5 SIWZ
4. W przypadku oferty składanej przez wykonawców ubiegających się wspólnie o udzielenie zamówienia publicznego, dokumenty potwierdzające, że wykonawca nie podlega wykluczeniu składa każdy z wykonawców oddzielnie.
5. 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, jak również Wykonawców którzy nie złożyli listy podmiotów należących do tej samej grupy kapitałowej lub informacji o tym, że nie należą do grupy kapitałowej , do ich złożenia w wyznaczonym terminie, chyba że mimo ich złożenia oferta Wykonawcy podlega odrzuceniu albo konieczne będzie unieważnienie postępowania.
6. 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.

VII.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. Wnioski należy kierować na adres zamawiającego lub e-mail zp@szpitalceglana.pl , nr fax 32-358-14-32
2. Oświadczenia, wnioski, zawiadomienia oraz informacje zamawiający i wykonawcy przekazują pisemnie, faksem lub drogą elektroniczną z zastrzeżeniem pkt. 3. 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. Tylko forma pisemna zastrzeżona jest dla złożenia oferty wraz z załącznikami, jak również dokumentów, oświadczeń ,pełnomocnictw uzupełnianych na podstawie art. 26.ust.3 ustawy Pzp.
4. Osoby uprawnione do porozumiewania się z wykonawcami: Andrzej Rechowicz Kierownik Działu Zamówień Publicznych, pok. E057, tel. 32-358-13-32 fax 32 358-14-32 e-mail : zp@szpitalceglana.pl w godzinach pracy od poniedziałku do piątku godz. 7.25 – 15.00.

VIII. WADIUM

Zamawiający nie wymaga wniesienia wadium.

IX. 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.

X. 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 w ofercie następujących dokumentów :

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 i nr 3 niniejszej specyfikacji.
c) Wypełniony, podpisany i opieczętowany przez osobę uprawnioną/ osoby uprawnione do reprezentowania wykonawcy formularz zawierający wymagane parametry jakościowe i techniczne przedmiotu zamówienia według druku stanowiącego załącznik nr 4.
d) Wypełniony, podpisany i opieczętowany przez osobę uprawnioną/ osoby uprawnione do reprezentowania wykonawcy formularz cenowy zawierający wyszczególnienie asortymentowe i ilościowe przedmiotu zamówienia według druku stanowiącego załącznik nr 7 SIWZ
e) Załączenie do oferty wymaganych przez Zamawiającego dokumentów , oświadczeń wyszczególnionych w pkt. VI

6. Dokumenty określone w pkt. VI 2b) 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 notarialnie.
8. Dla wykonawców występujących wspólnie ma w szczególności zastosowanie art. 23 Prawa zamówień publicznych. Wykonawcy wspólnie ubiegający się o zamówienie zobowiązani są do ustanowienia pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania ich w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo należy załączyć do oferty.
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
Samodzielny Publiczny Szpital Kliniczny Śląskiego Uniwersytetu Medycznego w Katowicach
ul. Ceglana 35 40-514 Katowice
„Oferta na dostawę licencji oprogramowania antywirusowego
D/ZP/381/63B/15
– Nie otwierać przed 28.08.2015r. godz.10.45"

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 Formularzu oferty części zamówienia, której wykonanie powierzy podwykonawcom.
13. Zamawiający żąda wskazania przez Wykonawcę nazw (firm) podwykonawców, na których zasoby Wykonawca powołuje się na zasadach określonych w art. 26 ust. 2b Pzp, w celu wykazania spełniania warunków udziału w postępowaniu, o których mowa w art. 22 ust. 1 Pzp.
14. Wszelkie poprawki lub zmiany w tekście oferty muszą być parafowane własnoręcznie przez osobę podpisującą ofertę.
15. Zamawiający nie ujawni informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli Wykonawca, nie później niż w terminie składania ofert zastrzeże, że nie mogą być one udostępniane oraz wykaże, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Przez tajemnicę przedsiębiorstwa rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą , co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności. Wykonawca nie może zastrzec swojej nazwy (firmy) oraz adresu, informacji dotyczących ceny, terminu wykonania zamówienia, warunków płatności zawartych w ofercie. Gdy informacje zawarte w ofercie stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji, winny być oznakowane klauzulą :,, Informacje stanowiące tajemnicę przedsiębiorstwa" i dołączone do oferty, zaleca się ,aby były trwale ,oddzielnie spięte.

XI. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT

Opakowaną w wyżej wymieniony sposób ofertę należy złożyć w Uniwersyteckim Centrum Okulistyki i Onkologii Samodzielnym Publicznym Szpitalu Klinicznym Śląskiego Uniwersytetu Medycznego w Katowicach przy ul. Ceglanej 35 w sekretariacie pokój **D022**

Termin składania ofert upływa w dniu <u>28.08.2015r. o godz.10.00.</u>
Zamawiający niezwłocznie zwróci oferty złożone po terminie składania ofert..

Otwarcie ofert nastąpi Uniwersyteckim Centrum Okulistyki i Onkologii Samodzielnym Publicznym Szpitalu Klinicznym Śląskiego Uniwersytetu Medycznego w Katowicach przy ul. Ceglanej 35 w pokoju E057 w dniu **<u>28.08.2015r. o godz. 10.45</u>**

XII. OPIS SPOSOBU OBLICZENIA CENY

1. Cena 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 np.:
   -koszty dostawy do Zamawiającego;
   -koszty cła i podatków, jeśli takie występują;
   - wszelkie opłaty i wynagrodzenia autorskie za dostarczone oprogramowanie wraz z licencjami
   - koszty wynikające z zapisów realizacji umowy stanowiącej załącznik nr 6 SIWZ
3. Wykonawca określa cenę realizacji zamówienia poprzez wypełnienie formularza asortymentowo-cenowego – załącznik nr 7 oraz przeniesienie do formularza oferty sumy cen netto elementów przedmiotu zamówienia, kwoty podatku VAT oraz ceny ofertowej z podatkiem VAT .
4. Cena ma być wyrażona w złotych polskich.
5. Ceny jednostkowe , ceny netto i brutto oraz należny podatek VAT należy podać z dokładnością do dwóch miejsc po przecinku.
6. Stawka podatku VAT jest określana zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2004 r. Nr 54, poz. 535 z późn.zm).

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

Kryterium oceny ofert jest :

Cena - 95%
5% - wydajność wg testu File Detection Test przeprowadzonego przez niezależną organizację AntiVirus –Comparative

<u>Sposób obliczania liczby punktów badanej oferty za cenę:</u>

C min. – cena minimalna spośród ocenianych ofert

Cn – cena badanej oferty
100 – stały współczynnik
(Cmin / Cn) x 100 x 95% = ilość punktów badanej oferty

Sposób obliczania liczby punktów badanej oferty za wydajność
wg testu File Detection Test przeprowadzonego przez niezależną organizację AntiVirus – Comparative

wynik na poziomie **ADVANCED** (III.2015) – **0 pkt**
wynik na poziomie **ADVANCED+**(III.2015) – **5 pkt**

Kryterium należy określić w formularzu ofertowym załącznik nr 1 wpisując odpowiednia TAK/NIE

Dla dokonania punktacji ofert, ranga w kryteriach oceny ofert określona w procentach, zostanie przeliczona na punkty 1 % = 1 punkt
Suma punktów uzyskanych przez Wykonawcę za w/w kryteria stanowić będzie ocenę końcową oferty.

Zamawiający za najkorzystniejszą uzna ofertę, złożoną przez Wykonawcę ,który łącznie uzyska najwyższą ilość punktów w w/w kryteriach.

XIV. 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, na warunkach będących istotnymi postanowieniami, a stanowiącymi wzór umowy – załącznik nr 6 do niniejszej specyfikacji. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem ww. terminu jeżeli w postępowaniu zostanie złożona tylko jedna oferta, a także, gdy w postępowaniu nie zostanie odrzucona żadna oferta oraz nie zostanie wykluczony żaden wykonawca. 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. Zamawiający zapłaci wynagrodzenie Wykonawcy, za dostarczone oprogramowanie w ciągu 30 dni od otrzymania faktury VAT wystawionej po podpisaniu Protokołu Odbioru .
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 2013 r. poz.907 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 i 3 Formularz oświadczeń wykonawcy
4. Wymagane i oferowane parametry jakościowe i techniczne przedmiotu zamówienia
5– Lista podmiotów należących do tej samej grupy kapitałowej lub oświadczenie o tym, że Wykonawca nie należy do grupy kapitałowej
6 - Wzór umowy
7 – Formularz asortymentowo cenowy

D/ZP/381/63B/15
Załącznik nr 1
.....
pieczęć firmowa wykonawcy

FORMULARZ OFERTOWY
DLA UNIWERSYTECKIEGO CENTRUM OKULISTYKI I ONKOLOGII
SAMODZIELNEGO PUBLICZNEGO SZPITALA KLINICZNEGO
ŚLĄSKIEGO UNIWERSYTETU MEDYCZNEGO W KATOWICACH

Nazwa wykonawcy .....

Siedziba: .....

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

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

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

Ubiegając się o zamówienie publiczne na **dostawę licencji oprogramowania antywirusowego** w ilości i asortymencie określonym w specyfikacji istotnych warunków zamówienia oferujemy realizację przedmiotowego zamówienia

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

Kryterium oceny ofert
Oferujemy : wydajność wg testu File Detection Test przeprowadzonego przez niezależną organizację AntiVirus – Comparative

wynik na poziomie ADVANCED (III.2015) ..... *(wpisać TAK lub NIE)*

wynik na poziomie ADVANCED+(III.2015) ..... *(wpisać TAK lub NIE)*

Termin dostawy:
Wykonawca w terminie 7 dni roboczych od daty zawarcia umowy udzieli Zamawiającemu licencji na Oprogramowanie,
wdroży Oprogramowanie **(*)** oraz przeszkoli trzech wskazanych przez Zamawiającego pracowników z zakresu obsługi Oprogramowania **(*)**.
Licencja zostanie udzielona na okres dwóch lat od daty podpisania Protokołu Odbioru Oprogramowania

Termin płatności: Zamawiający zapłaci wynagrodzenie Wykonawcy, za dostarczone oprogramowanie w ciągu 30 dni od otrzymania faktury VAT wystawionej po podpisaniu Protokołu Odbioru .

- 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
- Oświadczam , że następującą część zamówienia.....zamierzam powierzyć podwykonawcom
- Wskazuję następujących podwykonawców ..... **nazwa (firma)** ..... jako podmioty, na których zasoby powołuję się na zasadach określonych w art. 26 ust. 2b ustawy Prawo zamówień publicznych, w celu wykazania spełniania warunków udziału w postępowaniu, o których mowa w art. 22 ust. 1 tej ustawy;
- Znając treść art. 297 §1 Kodeksu Karnego oświadczamy, że dane zawarte w ofercie, dokumentach i oświadczeniach są zgodne ze stanem faktycznym.

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

D/ZP/381/63B/15
Załącznik nr 2

.....

pieczęć firmowa wykonawcy

OŚWIADCZENIA WYKONAWCY

Oświadczam, że :

zgodnie z art. 22 ust.1 ustawy Prawo zamówień publicznych spełniam 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/381/63B/15
Załącznik nr 3

.....
pieczęć firmowa wykonawcy

OŚWIADCZENIE WYKONAWCY

Oświadczam, że nie podlegam wykluczeniu z postępowania o udzielenie zamówienia publicznego na podstawie art. 24 ust.1 ustawy Prawo zamówień publicznych

.....

podpis i pieczęć osoby uprawnionej/osób uprawnionych
do reprezentowania wykonawcy

D/ZP/381/63B/15
Załącznik nr 4

.....
pieczęć firmowa wykonawcy

MINIMALNE WYMAGANIA DOTYCZĄCE DOSTAWY LICENCJI OPROGRAMOWANIA ANTYWIRUSOWEGO

1. Przedmiotem zamówienia jest dostawa i wdrożenie*****:
   - 330 licencji oprogramowania antywirusowego zabezpieczającego stacje robocze na okres 24 miesięcy
   - 10 licencji oprogramowania antywirusowego zabezpieczającego urządzenia mobilne tj. laptopy (systemy Windows), tablety (system Android), zabezpieczającego na okres 24 miesięcy
   - 3 licencji zabezpieczających serwery (System Linux, Windows Server) na okres 24 miesięcy
   - konsola centralnego zarządzania *

***UWAGA**: Zamawiający obecnie posiada pakiet antywirusowy ESET Endpoint Security Client dla stacji roboczych (w sumie 315 licencji) wraz z wdrożoną konsolą do centralnego zarządzania. W przypadku zaoferowania takiego samego pakietu antywirusowego Zamawiający nie wymaga dostawy konsoli centralnego zarządzania oraz wdrożenia dostarczonego oprogramowania.

2. Oprogramowanie to będzie używane na stacjach roboczych z systemami operacyjnymi takimi jak: Windows Vista, Windows 7, Windows 8/8.1 (systemy 32 i 64 bitowe) oraz na serwerach z systemami operacyjnymi takimi jak: Windows Serwer, Linux Suse, Linux Oracle.
3. Udzielona licencja powinna umożliwić użytkowanie programu Zamawiającego będącego samodzielnym publicznym zakładem opieki zdrowotnej, a także przez podmiot leczniczy w formie spółki kapitałowej, który powstanie w wyniku przekształcenia Zamawiającego oraz Samodzielnego Publicznego Centralnego Szpitala Klinicznego im. prof. K. Gibińskiego Śląskiego Uniwersytetu Medycznego w Katowicach przy ul. Medyków 14 w jedną spółkę kapitałową,
4. Użyte przez Zamawiającego wszelkie nazwy handlowe, znaki towarowe, patenty i miejsce pochodzenia są uzasadnione specyfiką przedmiotu zamówienia i mają na celu wskazanie jedynie jakości przedmiotu zamówienia.

Lp.	***Wymagania minimalne***
1.	***Wymagania ogólne dla stacji roboczych i laptopów:*** • Pełne wsparcie dla systemu Windows Vista/Windows 7/Windows 8/8.1 • Wsparcie dla 32- i 64-bitowej wersji systemu Windows • Wersja programu dla stacji roboczych Windows dostępna w całości w języku polskim • 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+ (XI 2014) - w teście Anti-Phishing Test na poziomie Advanced+ (VIII 2013) - w teście File Detecion Test na poziomie Advanced (III 2015) - w teście Performance Test na poziomie Advanced + (V 2015) - w pozostałych testach przynajmniej na poziomie Advanced
2.	***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, dysków sieciowych oraz nośników zewnętrznych 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. • 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. • 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. • 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. • 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. • Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik komputera 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. • Możliwość zabezpieczenia hasłem konfiguracji programu oraz jego nieautoryzowanej próby deinstalacji • 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. • System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. • Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych,pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych • 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: • tryb automatyczny z regułami gdzie aplikacja automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to aplikacja pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • 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. • Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, 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 wspierać technologię NetWork Access Protection (NAP). • Program ma wspierać technologię CISCO NetWork Access Control. • 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. • 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.
3	***Ochrona przed spamem:*** • Ochrona antyspamowa dla różnych programów pocztowych 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. • Integracja z różnymi programami pocztowymi - 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 zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam. • Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam. • 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.

4	***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.
5	***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.
6	***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 WindowsVista/Windows7/Windows 8 • 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 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 Vista/Windows7/Windows 8 oraz na serwerach /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 danych • Serwer centralnej administracji ma oferować administratorowi możliwość współpracy przynajmniej z trzema zewnętrznymi motorami baz danych w tym minimum z: Microsoft SQL Server, MySQL Server • 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 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.
7	***Ochrona serwer*ów** Wsparcie dla systemów: Microsoft Windows 2008, 2008 R2, 2012 R2 oraz systemu Linux • 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. • Możliwość skanowania dysków sieciowych i przenośnych • Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi. • Program powinien oferować możliwość skanowania dysków sieciowych typu NAS. • Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery

	producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika • System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. • Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.

WARUNKI LICENCJI

1. Wykonawca dostarczy licencję na oprogramowanie wraz ze wsparciem technicznym do wykorzystania w dowolnej jednostce organizacyjnej Szpitala. Wsparcie techniczne zapewnia Zamawiającemu dostęp do pomocy przy rozwiązywaniu problemów z dostarczonym Oprogramowaniem. Wsparcie techniczne ma być świadczone w języku polskim
2. Licencja zapewnia możliwość codziennej aktualizacji bazy sygnatur wirusów oraz aktualizacji samego oprogramowania.
3. W ramach dostarczonej licencji Wykonawca dostarczy nośnik z pakietem instalacyjnym
4. Wykonawca zobowiązany jest także dostarczyć instrukcję obsługi oprogramowania w języku polskim

INSTALACJA I WDROŻENIE *(jeżeli dotyczy)*

W przypadku dostarczenia programu antywirusowego innego niż obecnie używany przez Zamawiającego Wykonawca zobowiązany jest do:

- Instalacji i konfiguracji nowego Oprogramowania na stacjach roboczych wskazanych przez Zamawiającego
- Instalacji i konfiguracji konsoli centralnego zarządzania
- Przeszkolenia trzech wskazanych przez Zamawiającego pracowników z obsługi dostarczonego Oprogramowania

D/ZP/381/63B/15
Załącznik nr 5
.....
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. ……..

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

INFORMACJA WYKONAWCY , ŻE NIE NALEŻY DO GRUPY KAPITAŁOWEJ *

(o której mowa w art.24 ust.2 pkt 5 ustawy Prawo zamówień publicznych)

Informuję, że nie należę 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

*należy podpisać uzupełnioną listę lub informację

D/ZP/381/63B/15
Załącznik nr 7
.....
pieczęć firmowa wykonawcy

Formularz cenowy
Wyszczególnienie asortymentowe i ilościowe przedmiotu zamówienia

L.p.	Nazwa	Nazwa zaoferowanego oprogramowania	j.m.	Wymagana ilość	Cena jednostkowa	Wartość netto	Podatek VAT	Wartość brutto
1.	Licencja oprogramowania antywirusowego zabezpieczającego stacje robocze		licencja	**330**				
2.	Licencja oprogramowania antywirusowego zabezpieczającego urządzenia mobilne tj. laptopy (systemy Windows), tablety (system Android),		licencja	**10**				
3.	Licencja zabezpieczających serwery (System Linux, Windows Server)		licencja	**3**				
4.	*Jeżeli dotyczy* Konsola centralnego zarządzania		szt	**1**				
RAZEM:								

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

D/ZP/381/63B/15
Załącznik nr 6

UMOWA –wzór

Zawarta w dniu ..... w Katowicach pomiędzy:
Uniwersyteckim Centrum Okulistyki i Onkologii
Samodzielny Publiczny Szpital Kliniczny Śląskiego Uniwersytetu Medycznego w Katowicach
z siedzibą: 40 – 514 Katowice, ul. Ceglana 35
wpisanym do KRS pod nr 0000049660
NIP 954-22-74-017
REGON 001325767
zwanym w treści umowy Zamawiającym,
reprezentowanym przez:
Dariusza Jorg - Dyrektora Szpitala

……
z siedzibą: ……
wpisanym do ..... pod nr ……..
NIP
REGON
zwanym w treści umowy Wykonawcą
reprezentowanym 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 (tekst jednolity: Dz. U. z 2013 r. poz. 907 z późn.zm) została zawarta umowa następującej treści:

§ 1.
PRZEDMIOT UMOWY

5. Na podstawie oferty wybranej w/w postępowaniu Zamawiający zamawia**,** a Wykonawca zobowiązuje się :
   a) udzielić Zamawiającemu nieograniczonej na terytorium RP, 24 miesięcznej licencji na korzystanie z oprogramowania antywirusowego (zwanego dalej: „Oprogramowaniem")
   b) wdrożyć u Zamawiającego Oprogramowanie), **(*)**
   c) przeszkolić w zakresie obsługi dostarczonego Oprogramowania trzech wskazanych przez Zamawiającego pracowników) **(*)**
   d) dostarczyć w ramach Oprogramowania, zainstalować i skonfigurować konsole centralnego zarządzania) **(*)**
   e)zapewnić wsparcie techniczne dla Oprogramowania w zakresie i przez okres określony w umowie
6. Wdrożenie Oprogramowania polegać będzie na jego zainstalowaniu i uruchomieniu na stacjach roboczych wskazanych przez Zamawiającego oraz zainstalowaniu, skonfigurowaniu i uruchomieniu konsoli do zdalnego zarządzania Oprogramowaniem.
7. W załączniku nr 1 do umowy została określona nazwa i wersja Oprogramowania, którego minimalne parametry jakościowe i techniczne zostały określone w załączniku nr 4 do Specyfikacji Istotnych Warunków Zamówienia.

§ 2.
WARUNKI REALIZACJI UMOWY

1. Wykonawca zobowiązuje się do zrealizowania umowy zgodnie z warunkami określonymi w Specyfikacji Istotnych Warunków Zamówienia oraz w niniejszej umowie.
2. Wykonawca oświadcza i gwarantuje, że realizacja niniejszej umowy nie naruszy żadnych praw osób trzecich oraz że nie zachodzą żadne podstawy do zgłaszania z tytułu niniejszej umowy przez osoby trzecie wobec Zamawiającego jakichkolwiek roszczeń, a w szczególności z prawami własności intelektualnej (prawa autorskie, prawa własności przemysłowej). W przypadku gdyby osoba trzecia zgłosiła jakiekolwiek roszczenia wobec Zamawiającego dotyczące naruszenia jej praw w związku z niniejszą umową Wykonawca zobowiązuje się bez dodatkowego wynagrodzenia do udzielenia Zamawiającemu wszelkiej pomocy w obronie przed takimi roszczeniami, a w przypadku gdyby taka obrona nie była możliwa lub skuteczna Wykonawca zobowiązuje się zwolnić Zamawiającego z odpowiedzialności oraz pokryć Zamawiającemu wszelkie szkody związane z takimi roszczeniami.
3. Wykonawca w terminie 7 dni roboczych od daty zawarcia umowy udzieli Zamawiającemu licencji na Oprogramowanie, wdroży Oprogramowanie **(*)** oraz przeszkoli trzech wskazanych przez Zamawiającego pracowników z zakresu obsługi Oprogramowania **(*)**. Udzielona licencja musi zapewniać możliwość codziennej aktualizacji bazy struktur wirusów oraz możliwość bieżącego aktualizowania Oprogramowania. Licencja zostaje udzielona na okres dwóch lat od daty podpisania Protokołu Odbioru Oprogramowania

4. Wykonanie obowiązków Wykonawcy związanych z należytym uruchomieniem Oprogramowania zostanie potwierdzone Protokołem Odbioru Oprogramowania podpisanym przez obie Strony. Podpisanie Protokołu Odbioru przez Zamawiającego bez zastrzeżeń oznaczać będzie zrealizowanie umowy w zakresie udzielenia Zamawiającemu licencji na Oprogramowanie , wdrożenia Oprogramowania **(*)** oraz przeszkolenia trzech wskazanych przez Zamawiającego pracowników z zakresu obsługi Oprogramowania **(*)**.
5. W ramach realizacji niniejszej umowy Wykonawca bez dodatkowego wynagrodzenia dostarczy Zamawiającemu nośnik zawierający pakiet instalacyjny oraz pozostałe oprogramowanie niezbędne do poprawnego działania Oprogramowania oraz instrukcję obsługi Oprogramowania w języku polskim.
6. W ramach wynagrodzenia określonego w niniejszej umowie Wykonawca zapewni także wsparcie techniczne dla Oprogramowania. Zakres udzielonego wsparcia musi obejmować minimum świadczenie pomocy w zakresie rozwiązywania problemów dotyczących korzystania z Oprogramowania (konsultacje telefoniczne oraz poprzez Internet e-mail, pomoc zdalna) .
7. Udzielona licencja na Oprogramowanie musi zapewniać możliwość korzystania z Oprogramowania przez następcę prawnego Zamawiającego w przypadku przekształcenia Zamawiającego.

§ 3

GWARANCJE

1. Na dostarczone Oprogramowanie Wykonawca udziela Zamawiającemu gwarancji na okres 24 miesięcy od dnia podpisania Protokołu Odbioru o którym mowa w § 2 ust. 4.

2. Wykonawca zapewni Zamawiającemu możliwość zgłaszania wad, usterek nieprawidłowego działania Oprogramowania (awarie) w godzinach pracy Zamawiającego (od 7:00 do 15:00) od poniedziałku do piątku. Zgłoszenia wad, usterek i awarii 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 24 godzin od chwili zgłoszenia awarii.

§ 4

WYNAGRODZENIE I WARUNKI PŁATNOŚCI

1. Wynagrodzenie Wykonawcy za zrealizowanie całej umowy , zgodnie ze złożoną ofertą nie może przekroczyć kwoty: (osobno w zależności od uzyskanych części)
   brutto:.....zł (słownie:.....)
   netto: .....zł należny podatek VAT :.....zł
2. Zamawiający zapłaci Wykonawcy wynagrodzenie o którym mowa w ust.1 w ciągu 30 dni od otrzymania faktury VAT wystawionej po podpisaniu Protokołu Odbioru bez zastrzeżeń. W przypadku gdyby Wykonawca zamieścił na fakturze inny termin płatności niż określony w niniejszej umowie obowiązuje termin płatności określony w umowie.
3. Za datę zapłaty przyjmuje się datę obciążenia rachunku bankowego Zamawiającego.

§ 5

KARY UMOWNE

1. Wykonawca zapłaci Zamawiającemu kary umowne:
   a) w wysokości 0,2 % kwoty wynagrodzenia brutto określonego w § 4 ust. 1 za każdy dzień opóźnienia w realizacji któregokolwiek z obowiązków określonych w § 2 ust. 3 umowy
   b) w wysokości 10% kwoty wynagrodzenia brutto 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.

ZINTEGROWANY SYSTEM ZARZĄDZANIA

1. W związku z wdrożeniem przez Zamawiającego Zintegrowanego Systemu Zarządzania w zakresie zarządzania środowiskowego (norma ISO14001:2004) oraz zarządzania bezpieczeństwem i higieną pracy (norma OHSAS 18001:2007):
   a) Wykonawca gwarantuje, że osoby wykonujące usługę związaną z realizacją umowy posiadają wszystkie wymagane obowiązującymi przepisami oraz niezbędne dla realizacji umowy szkolenia z zakresu bezpieczeństwa i higieny pracy oraz aktualne badania lekarskie i specjalistyczne.
   b) Wykonawca gwarantuje, że osoby wykonujące usługę związaną z realizacją umowy przebywające na terenie Szpitala będą posiadały widoczne oznakowanie z logo firmy (np. identyfikatory i/lub ubranie robocze z widocznym napisem nazwy firmy).
   c) Wykonawca świadomy zagrożeń wynikających z działalności Zamawiającego (**załącznik A)** zobowiązuje się do podpisania wraz z umową następujących dokumentów:
   -**załączniki B** (Zobowiązanie Wykonawcy)

-załącznik C (Lista pracowników Wykonawcy poinformowanych o zagrożeniach wynikających z działalności Uniwersyteckiego Centrum Okulistyki i Onkologii w Katowicach)
-**załącznik D** (Zasady środowiskowe dla Wykonawców).

§ 7.

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 Wykonawca opóźni się z realizacją obowiązków określonych w § 2 ust. 3 umowy o ponad 14 dni kalendarzowych.
3. Oświadczenie Zamawiającego o odstąpieniu lub 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.

§ 8.

POSTANOWIENIA KOŃCOWE

1. Umowa zawarta jest na czas określony do dnia upływu okresu, na który została zgodnie z umową udzielona licencja na Oprogramowanie.
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. Strony dopuszczają możliwość podwyższenia wynagrodzenia należnego Wykonawcy wyłącznie w formie pisemnego aneksu do niniejszej umowy. Zmiana taka może nastąpić w przypadku zaistnienia przynajmniej jednej z następujących okoliczności:
   a) zmiany stawki podatku od towarów i usług,
   b) zmiany wysokości minimalnego wynagrodzenia za pracę ustalonego na podstawie art. 2 ust. 3-5 ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę,
   c) zmiany zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne
   pod warunkiem, że zmiany takie będą miały wpływ na koszty wykonania zamówienia przez Wykonawcę.
   W przypadku zaistnienia powyższych okoliczności Strona zamierzająca uzyskać zmianę wysokości wynagrodzenia zobowiązana jest do złożenia drugiej Stronie pisemnego wniosku o wprowadzenie stosownej zmiany. Wniosek o zmianę wynagrodzenia musi zawierać:
   a) wskazanie okoliczności stanowiącej podstawę do zmiany
   b) uzasadnienie wskazujące jaki wpływ ma okoliczność na wysokość wynagrodzenia wykonawcy,
   c) propozycję nowej wysokości wynagrodzenia.
   Na skutek złożonego, kompletnego wniosku spełniającego wymagania określone powyżej Strony w terminie 10 dni podejmą negocjacje dotyczące nowej wysokości wynagrodzenia. W przypadku uzgodnienia nowej wysokości wynagrodzenia Strony zawrą stosowny pisemny aneks do umowy.
8. Jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby wykonawca powoływał się , w celu wykazania spełniania warunków udziału w postępowaniu, Wykonawca jest obowiązany wykazać Zamawiającemu ,iż proponowany inny podwykonawca lub wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż wymagany w trakcie postepowania o udzielenie zamówienia.
9. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, dwa egzemplarze dla Zamawiającego, jeden egzemplarz dla Wykonawcy.

Załączniki do umowy:
1. Formularz cenowy zaoferowanego oprogramowania
2. Załączniki A,B,C,D

Wykonawca

Zamawiający

UWAGA: zapisy projektu umowy oznaczone (*) dotyczą wyłącznie przypadku dostarczenia oprogramowania równoważnego do obecnie posiadanego przez Zamawiającego

D/ZP/381/63B/15
Załącznik A

Informacja dla Wykonawcy o zagrożeniach wynikających z działalności Uniwersyteckiego Centrum Okulistyki i Onkologii w Katowicach podczas wykonywania prac na jego terenie.

CZYNNIKI BIOLOGICZNE

Lp.	*Zagrożenie*	*Skutek*	*Środki zapobiegawcze*
1.	Na terenie Szpitala występują szkodliwe czynniki biologiczne, które mogą oddziaływać negatywnie na organizm człowieka i być przyczyną wielu chorób (np. wirusowe zapalenie wątroby typ B i C, gruźlica, HIV). Podstawowym źródłem zagrożenia jest pacjent i jego materiał biologiczny. Sytuacje, w których może dojść do kontaktu z czynnikiem biologicznym 1. Niezabezpieczony przez personel medyczny skażony sprzęt i narzędzia jednorazowego lub wielorazowego użytku (igły, skalpele, igły do szycia itp.). 2. Nieodpowiednia segregacja zużytego sprzętu jednorazowego użytku. 3. Nieprawidłowa dekontaminacja miejsc zabrudzonych czynnikiem biologicznym. 4. Prace wykonywane na czynnej instalacji kanalizacyjnej (węzły sanitarne, kratki ściekowe, odstojniki, osadniki itp.). 5. Czynniki biologiczne przenoszone drogą powietrzno – kropelkową w kontakcie z pacjentami, odwiedzającymi oraz personelem Szpitala. 6. Czynniki biologiczne znajdujące się na powierzchniach, wyposażeniu, powierzchniach roboczych, sprzęcie medycznym.	Choroby zakaźne. Alergie, uczulenia, zakażenie. Choroby nowotworowe. Śmierć.	1. Skaleczenia, zranienia, otarcia przed przystąpieniem do pracy zabezpiecz opatrunkiem nieprzemakalnym. 2. Skaleczenia, zadrapania na odkrytych częściach rąk, ramion osłoń ubraniem z długim rękawem. 3. Zgłoś się do Izby Przyjęć w przypadku zakłucia, skaleczenia sprzętem i aparaturą medycznym, która potencjalnie może być skażoną krwią lub innym materiałem biologicznym. 4. W zależności od potrzeby stosuj środki ochrony indywidualnej (np. maseczki, okulary ochronne, przyłbice, rękawice). 5. Przestrzegaj podstawowych zasad higieny i bezpieczeństwa pracy myj i dezynfekuj ręce przed spożywaniem posiłku oraz po wyjściu ze Szpitala.

CZYNNIKI CHEMICZNE

Lp.	*Zagrożenie*	*Skutek*	*Środki zapobiegawcze*
2.	W Szpitalu podczas procesów pracy stosowane są niebezpieczne substancje i mieszaniny chemiczne takie jak: Odczynniki analityczne (kwasy, zasady) 2. Metanol, Ksylen 3. Formaldehyd 4. Podchloryn sodu 5. Tlenek etylenu 6. Środki dezynfekcyjne, myjące.	Zatrucia, podrażnienie. Choroby górnych dróg oddechowych. Alergie, uczulenia. Uszkodzenia oczu i skóry. Poparzenia.	1. Uzyskaj informację od personelu o stosowanych środkach chemicznych i zagrożeniach z nimi związanymi. 2. Zapoznaj się z właściwościami preparatów chemicznych, z którymi będziesz miał kontakt. 3. Postępuj zgodnie z zasadami określonymi w kartach charakterystyki i stosuj środki ochrony indywidualnej. 4. W sytuacjach awaryjnych (np. uszkodzenie opakowania, rozlanie środka chemicznego) poinformuj personel.

CZYNNIKI NIEBEZPIECZNE - URAZOWE

Lp.	*Zagrożenie*	*Skutek*	*Środki zapobiegawcze*
3.	W Szpitalu podczas procesów pracy używany jest sprzęt medyczny jednorazowego oraz wielorazowego użytku (np. igły, skalpele, wenflony, nożyczki, końcówki pipet, szkiełka), który może stanowić zagrożenie dla Wykonawcy i być przyczyną urazów. Do kontakt z tym sprzętem może dojść w sposób niezamierzony w przypadku nieprzestrzegania zasad segregacji przez personel medyczny oraz porzucenia przez pacjentów.	Rany cięte, kłute palców, dłoni. Skaleczenia. Przecięcia, zakłucia.	1. Nie podejmuj samodzielnie usuwania sprzętu i narzędzi medycznych pozostawionych przez personel lub pacjentów, zgłaszaj ten fakt personelowi medycznemu. 2. Zachowaj szczególną uwagę przy pracy z użyciem ostrych, spiczastych narzędzi.
4.	Podczas poruszania się po terenie Szpitala może dojść do: 1. Uderzenie o ruchome lub nieruchome czynniki materialne (np. wyposażenie pomieszczeń, meble, aparatura i sprzęt medyczny, łóżka, wózki z pacjentami na salach, korytarzach, ciągach komunikacyjnych itp.). 2. Upadku na tym samym poziomie spowodowanym potknięciem, poślizgnięciem na nierównych, mokrych, śliskich powierzchniach. 3. Upadku na schodach.	Potłuczenia, guzy, siniaki. Złamania kończyn. Uszkodzenia kręgosłupa. Wstrząśnięcia mózgu.	1. Utrzymuj porządek i czystość na stanowisku pracy. 2. Poruszaj się po drogach komunikacyjnych stosując zasadę poruszania się prawą stroną. 3. Zwracaj uwagę na transportowanych pacjentów na wózkach i łóżka na ciągach komunikacyjnych. 4. Zachowaj uwagę podczas poruszania się po schodach: nie rozmawiaj przez telefon, nie używaj klatki schodowej jako drogi transportowej, trzymaj się poręczy.

D/ZP/381/63B/15
Załącznik B

Zobowiązanie Wykonawcy

W imieniu Wykonawcy realizującego przedmiot umowy nr …… z dnia ……. („Umowa”) zobowiązuję się do:

1. Przestrzegania ogólnie obowiązujących przepisów i zasad w zakresie bezpieczeństwa i higieny pracy, ochrony przeciwpożarowej oraz ochrony środowiska, jakich dotyczy zakres świadczonych prac lub usług.
2. Zapoznania swoich pracowników oraz pracowników podwykonawcy delegowanych do realizacji Umowy z treścią niniejszej procedury nie później niż przed rozpoczęciem realizacji Umowy.
3. Poinformowania swoich pracowników oraz pracowników podwykonawcy o zagrożeniach wynikających z działalności Szpitala nie później niż przed rozpoczęciem prac i usług objętych Umową.

Ze strony Uniwersyteckiego Centrum Okulistyki i Onkologii w Katowicach:

……..…….……...

osoba sprawująca nadzór

Wykonawca ……..……...……

nazwa firmy

…..…….……

adres

W imieniu Wykonawcy**:**

Nazwisko, imię ……..…….……

Stanowisko / funkcja ……..

…….. ……..

Data Podpis

D/ZP/381/63B/15
Załącznik C

Lista pracowników Wykonawcy
poinformowanych o zagrożeniach wynikających z działalności
Uniwersyteckiego Centrum Okulistyki i Onkologii w Katowicach

Nazwa firmy:

Inwestycja: Umowa nr ……. z dnia …….

Lp.	Imię i Nazwisko	Stanowisko	Data	Podpis
1.				
2				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16				
17.				
18				
19.				
20.				

Podpis Wykonawcy

…….

D/ZP/381/63B/15
Załącznik D

ZASADY ŚRODOWISKOWE DLA WYKONAWCÓW

1. Wykonawca powinien przestrzegać wymagań określonych w systemie zarządzania środowiskowego wg. ISO14001, a w szczególności:
   - przestrzegać wymagań prawnych w zakresie podpisanej ze Szpitalem umowy
   - zmniejszyć dla otoczenia uciążliwość swojej działalności związanej z wykonywaniem prac zleconych przez Szpital
   - minimalizować ilość powstających odpadów
   - zabierać z terenu wszelkie odpady powstałe w czasie świadczenia usług
   - zmniejszać zużycie nośników energii i surowców naturalnych

2. Wykonawcy nie wolno:
   - wwozić na teren Szpitala jakichkolwiek odpadów
   - składować żadnych substancji mogących zanieczyścić powietrze atmosferyczne, wodę, glebę, a w przypadku, gdy substancje te służą do wykonywania usług dla firmy szczegóły ich składowania i stosowania należy uzgodnić z Koordynatorem ds. środowiska
   - myć pojazdów na terenie Szpitala
   - spalać odpadów na terenie Szpitala
   - wylewać jakichkolwiek substancji niebezpiecznych do gleby lub kanalizacji

3. Wykonawca powinien przeprowadzić szkolenie wśród podległych pracowników wykonujących usługę w zakresie obowiązującej w Szpitalu polityki środowiskowej, bhp oraz systemu zarządzania środowiskowego wg ISO 14001.

4. Wykonawca powinien dopuścić Pełnomocnika ds. Jakości wraz z zespołem auditorów do kontroli postępowania na zgodność z przyjętymi zasadami środowiskowymi w Szpitalu.

5. W sytuacjach wątpliwych i nieokreślonych w powyższych zasadach środowiskowych należy zwracać się do Pełnomocnika ds. Jakości.

Podpis Wykonawcy

…….

.....
data