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

Znak sprawy : D/ZP/381/101B/15

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

Na dostawę sprzętu komputerowego

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 26.11.2015r.

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

mgr Andrzej Rechowicz
Kierownik Działu Zamówień Publicznych

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. Dostawa sprzętu komputerowego - wyszczególnionego asortymentowo i ilosciowo w załączniku nr od 5.1 do 5.3 siwz o parametrach jakościowych i technicznych opisanych w załaczniku nr 4.1 do 4.3 siwz
   Część 1 – Zestawy komputerowe
   Część 2 – Komputery przenośne
   Część 3 – Czytniki kart chipowych
2. Dostarczony sprzęt komputerowy musi być fabrycznie nowy, nie starszy niż 6 miesięcy od daty produkcji, pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski i posiadać wszystkie wymagane prawem certyfikaty lub dokumenty równoważne,
3. Nazwy i kody wg Wspólnego Słownika Zamówień:
   30.21.33.00-8 – komputer biurkowy
   30.23.12.00-0 monitory ekranowe
   30.21.31.00-6- komputery przenośne
   30.23.60.00-2 różny sprzęt komputerowy
4. Zamawiający dopuszcza możliwość składania ofert częściowych - na dowolną ilość części przy czym części nie mogą być dzielone przez Wykonawców.
5. Przedmiot i warunki realizacji niniejszego zamówienia winny być zgodne z obowiązującymi przepisami prawnymi w tym zakresie.
6. Wykonawca dostarczy Zamawiającemu razem ze sprzętem komputerowym:
   - dokumenty gwarancyjne,
   - inne wymagane prawem dokumenty.
7. Wymagania Zamawiającego dotyczące gwarancji i serwisu :
   a) Minimalne wymagania Zamawiającego dotyczące okresu gwarancji podano w załączniku nr 4.1 - 4.3 do SIWZ.
   b) W okresie gwarancji Wykonawca jest zobowiązany nieodpłatnie dokonać naprawy lub wymiany sprzętu lub jego poszczególnych części - także w przypadku, gdy konieczność naprawy lub wymiany jest wynikiem eksploatacyjnego zużycia sprzętu lub jego części.
   c) Wykonawca gwarantuje naprawę uszkodzonego sprzętu komputerowego , albo wymianę sprzętu lub jego części na nowe w terminie liczonym od zgłoszenia awarii nie dłuższym niż 7 dni roboczych (część 1) i 14 dni roboczych (część 2 i 3)
   d) W przypadku naprawy sprzętu komputerowego trwającej dłużej niż określono w pkt.7c) , Wykonawca zobowiązany jest nieodpłatnie dostarczyć na okres przedłużającej się naprawy sprawne urządzenie zastępujące w pełni urządzenie naprawiane.
   e) W przypadku, gdy liczba napraw gwarancyjnych przekroczy 3 naprawy tego samego urządzenia lub podzespołu Wykonawca zobowiązany jest do wymiany urządzenia na nowe (z wyjątkiem uszkodzeń z winy użytkownika). Wymiana urządzenia lub podzespołu nastąpi w terminie określonym w pkt.7c).
   f) W przypadku awarii i konieczności zabrania sprzętu komputerowego z siedziby Zamawiającego jak również w przypadku konieczności wymiany uszkodzonej pamięci masowej (dysków) w ramach naprawy gwarancyjnej dysk twardy podlegający wymianie pozostaje własnością Zamawiającego.
   g) Okres gwarancji udzielonej przez Wykonawcę ulega przedłużeniu o pełen okres niesprawności dostarczonego urządzenia.

IV. TERMIN WYKONANIA ZAMÓWIENIA:

Dostawa sprzętu komputerowego w terminie do… (*zgodnie z zaoferowanym terminem dostawy w ofercie – kryterium oceny ofert*) dni kalendarzowych od dnia zawarcia 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

a) posiadania uprawnień do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania - Zamawiający nie stawia szczegółowych warunków - za spełniających te warunki Zamawiający uzna Wykonawców, którzy przedłożą oświadczenie o spełnianiu warunków udziału w postępowaniu.

b) posiadania wiedzy i doświadczenia - Zamawiający nie stawia szczegółowych warunków - za spełniających te warunki Zamawiający uzna Wykonawców, którzy przedłożą oświadczenie o spełnianiu warunków udziału w postępowaniu.

c) dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia – Zamawiający nie stawia szczegółowych warunków - za spełniających te warunki Zamawiający uzna Wykonawców, którzy przedłożą oświadczenie o spełnianiu warunków udziału w postępowaniu.

d) 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.

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 o spełnianiu warunków udziału w postepowaniu 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 oświadczenie o tym, że nie należy do grupy kapitałowej – załącznik nr 6 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 lub 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, fax 32 3581-432 e-mail : zp@szpitalceglana.pl

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 PRZYGOTOWANIA OFERTY

1. Wykonawca ponosi wszelkie koszty przygotowania i złożenia oferty.
2. Każdy wykonawca może złożyć tylko jedną ofertę na dowolną ilość części .
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 na drukach (odpowiednio do oferowanej/nych części) stanowiących załącznik nr 4.1 lub/ i załącznik nr 4.2 lub/ i załącznik nr 4.3.

d) Wypełniony, podpisany i opieczętowany przez osobę uprawnioną/ osoby uprawnione do reprezentowania wykonawcy formularz cenowy zawierający wyszczególnienie asortymentowe i ilościowe przedmiotu zamówienia na drukach (odpowiednio do oferowanej/nych części) stanowiących załącznik nr 5.1 lub/ i załącznik nr 5.2 lub/ i załącznik nr 5.3 .

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. Warunki określone w art. 22 ust. 1 pkt 2 i 3 Prawa zamówień publicznych mogą być spełnione przez jednego z członków konsorcjum lub wszystkich uczestników konsorcjum łącznie. 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 sprzętu komputerowego część …….

D/ZP/381/101B/15
– Nie otwierać przed 04.12.2015r. 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 oferty 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 zastrzegł, 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, okresu gwarancji i warunków płatności zawartych w ofercie.

XI. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT

Opakowaną w wyżej wymieniony sposób ofertę należy złożyć w Uniwersyteckim Centrum Okulistyki i Onkologii Samodzielny Publiczny Szpital Kliniczny Śląskiego Uniwersytetu Medycznego w Katowicach przy ul. Ceglanej 35 w sekretariacie pokój **D022**

Termin składania ofert upływa w dniu 04.12.2015.r o godz.10.00.
Zamawiający niezwłocznie zwróci oferty złożone po terminie składania ofert..

Otwarcie ofert nastąpi Uniwersyteckim Centrum Okulistyki i Onkologii Samodzielny Publiczny Szpital Kliniczny Śląskiego Uniwersytetu Medycznego w Katowicach przy ul. Ceglanej 35 w pokoju E057 w dniu **04.12.2015r. o godz. 10.30**

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 miejsca wskazanego przez Zamawiającego;
   - koszty ubezpieczenia dostawy do Zamawiającego
   - koszty cła i podatków, jeśli takie występują;
   - wszelkie opłaty i wynagrodzenia autorskie za dostarczone licencje
   - koszty związane z udzieleniem gwarancji i serwisu na sprzęt komputerowy
   - koszty dostarczenia sprzętu zastępczego jeżeli wystąpią okoliczności opisane w SIWZ
2. Zamawiający wymaga, aby cena w formularzu cenowym była obliczana w następujący sposób:
   - cena jednostkowa netto: cena zaoferowana przez Wykonawcę za jednostkę miary
   - wartość netto: iloczyn ceny jednostkowej netto i wymaganej ilości
   - podatek VAT : wyrażona w złotówkach lub % wartość należnego podatku VAT
   - wartość brutto: suma wartości netto i podatku VAT.

   Cena ofertowa brutto to zsumowana wartość brutto wszystkich pozycji przedmiotu zamówienia dla oferowanej części.
3. Wykonawca określa cenę realizacji zamówienia poprzez wypełnienie formularza asortymentowo-cenowego oraz przeniesienie do formularza oferty cen netto elementów przedmiotu zamówienia, kwoty podatku VAT oraz ceny ofertowej z podatkiem VAT dla każdej oferowanej części zamówienia
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 dla każdej zaoferowanej części z osobna jest :

Cena - 95%
Termin dostawy – 5%
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 95% = ilość punktów badanej oferty

Sposób obliczania liczby punktów badanej oferty za termin dostawy :

Termin dostawy określić należy w dniach kalendarzowych w formularzu ofertowym dla oferowanych części – załącznik nr 1 Specyfikacji istotnych warunków zamówienia . Dla każdej części może być zaoferowany inny termin dostawy lub dla wszystkich części taki sam .

termin dostawy określony w dniach kalendarzowych punktowany będzie w następujący sposób :
15 dni kalendarzowych - 5 punktów

20 dni kalendarzowych – 3 punkty
25 dni kalendarzowych – 2 punkty
30 dni kalendarzowych – 0 punktów

maksymalnym terminem dostawy, który może zostać zaoferowany w ofercie jest 30 dni kalendarzowych

Oferty z terminem dostawy powyżej 30 dni kalendarzowych Zamawiający odrzuci na podstawie art. 89 ust.1 pkt 2) jako niezgodne ze specyfikacją istotnych warunków zamówienia.

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 w danej części uzyska najwyższą ilość punktów 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 7 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 dostarczony sprzęt komputerowy 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
4.1 - 4.3 - Wymagane i oferowane parametry jakościowe i techniczne przedmiotu zamówienia
5.1- 5.3 - Formularze cenowe wyszczególnienie asortymentowe i ilościowe
6 – Lista podmiotów należących do tej samej grupy kapitałowej lub oświadczenie o tym, że Wykonawca nie należy do grupy kapitałowej
7 - Wzór umowy

D/ZP/381/101B/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 **sprzętu komputerowego** w ilości i asortymencie określonym w specyfikacji istotnych warunków zamówienia oferujemy realizację przedmiotowego zamówienia

Część 1 – Zestawy komputerowe
za cenę netto ..... zł
podatek VAT .....% tj. ..... zł
Cena ofertowa z podatkiem VAT: .....zł
(słownie:.....zł)

Część 2 – Komputery przenośne
za cenę netto ..... zł
podatek VAT .....% tj. ..... zł
Cena ofertowa z podatkiem VAT: .....zł
(słownie:.....zł)

Część 3 –Czytniki kart chipowych
za cenę netto ..... zł
podatek VAT .....% tj. ..... zł
Cena ofertowa z podatkiem VAT: .....zł
(słownie:.....zł)

Termin dostawy:
Dostawa sprzętu komputerowego w terminie do:
dla części nr **.....**do *(wpisać oferowany termin dostawy- **15,20,25,30** - **kryterium oceny ofert**)* **.....** dni kalendarzowych od dnia zawarcia umowy.

Warunki gwarancji i serwisu określono w załączniku nr 4.1 - 4.3 specyfikacji istotnych warunków zamówienia

Termin płatności: Zamawiający zapłaci wynagrodzenie Wykonawcy, za dostarczony sprzęt komputerowy 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/381/101B/15
Załącznik nr 2

.....

pieczęć firmowa wykonawcy

<u>OŚWIADCZENIA WYKONAWCY</u>

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/381/101B/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/381/101B/15
Załącznik nr 4.1
.....
pieczęć firmowa wykonawcy

WYMAGANE i OFEROWANE PARAMETRY JAKOŚCIOWE i TECHNICZNE PRZEDMIOTU ZAMÓWIENIA
Część 1 – ZESTAWY KOMPUTEROWE
(ilość 15 kompletów)

Lp.	Wymagania minimalne	Czy spełnia ?
1	**2**	**3**
1	Przeznaczenie	----------
A	Praca sieciowa w aplikacji bazodanowej z wykorzystaniem m.in. aplikacji webowych	
B	Praca na aplikacjach biurowych, m.in. pakiet Microsoft Office w wersji od 2010 w wzwyż, pakiet Open Office w wersji 4.x	
C	Praca z wykorzystaniem przeglądarek internetowych m.in. Internet Explorer w wersji 10 i w wzwyż, Mozilla Firefox w wersji 38.x i w wzwyż i innych	
2	Wymagane parametry techniczne:	----------
A	Pamięć operacyjna minimum 8GB typu DDR3 (w jednej kości) z możliwością rozbudowy do minimum 16GB tylko poprzez dołożenie kolejnego modułu pamięci	podać ile: ……
B	Interfejs sieciowy Ethernet 10/100/1000BaseTX (sterowniki do karty sieciowej muszą umożliwiać konfiguracji parametrów do obsługi VLAN (tagowanych, nietagowych) poprzez tworzenie kolejnych wirtualnych połączeń sieciowych na jednej fizycznej karcie sieciowej)	podać model: ……
C	Karta graficzna pracująca w trybie Full HD z pamięcią przydzielaną dynamicznie do 1692MB, o rozdzielczości nominalnej 1440x900 pikseli, umożliwiająca obsługę 3 monitorów jednocześnie	podać model: ……
D	Pamięć masowa o pojemności minimum 500GB i prędkości obrotowej minimum 7200rpm typu hybrydowego SSHD	podać ile: …… podać typ ……
E	Zintegrowana karta dźwiękowa	
F	Napęd optyczny DVD-RW wraz z oprogramowaniem do zastosowania w celach komercyjnych	Podać nazwę oprogramowania: ……..
G	Zasilacz o sprawności energetycznej do 85% (certyfikat 80 PLUS Bronze), zgodny z normą ENERGY STAR 6.0	
3	Wymagana funkcjonalność:	
A	Wydajność obliczeniowa komputera na podstawie testów aplikacyjnych SYSmark2014 (www.bapco.com): w teście SYSmark 2014 Overall minimum 1567 pkt, w teście SYSmark 2014 Office Productivity minimum 1325 pkt, w teście SYSmark 2014 Data/Financial Analysis minimum 1782 pkt.	
B	Obudowa typu SFF/USFF	
C	Zgodność z systemami operacyjnymi i standardami potwierdzona certyfikatem WHCL oraz certyfikatem CE	
D	Złącza zewnętrzne minimum: słuchawkowe, mikrofonowe, USB2.0 4 sztuki, USB3.0 4 sztuki, RJ45 1 sztuka, D-Sub 1 sztuka, DisplayPort 2 sztuki,	
E	Możliwość odczytania z BIOS: (wersji BIOS, modelu procesora wraz z informacjami o ilości rdzeni, prędkościach min i max zegara, wielkości podręcznej pamięci Cache, informacji o ilości pamięci RAM, informacji o dysku twardym)	
F	Możliwość wyłączenia zintegrowanej(nych) karty sieciowej, możliwość wyłączenia portów USB z poziomu BIOS bez uruchamiania systemu operacyjnego komputera	
G	Funkcja blokowania/odblokowywania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania	

	systemu operacyjnego	
H	Możliwość ustawienia hasła na poziomie administratora bez potrzeby uruchamiania systemu operacyjnego	
I	Nie dopuszcza się stosowania tzw. overclockingu w celu uzyskania wymaganych parametrów pracy zestawu komputerowego	
4	Wyposażenie dodatkowe:	----------
A	Zainstalowany system operacyjny w wersji do zastosowań komercyjnych, profesjonalnych wg wymagań wyszczególnionych w dalszej części siwz wraz z nośnikiem instalacyjnym na płycie DVD i licencją dożywotnią	
B	Zainstalowany pakiet antywirusowy w wersji do zastosowań komercyjnych, profesjonalnych wg wymagań wyszczególnionych w dalszej części siwz	
C	Klawiatura USB w układzie polski programisty tego samego producenta co komputer lub certyfikowana przez producenta komputera	
D	Mysz optyczna USB z minimum dwoma przyciskami i rolka (scroll) tego samego producenta, co komputer lub certyfikowana przez producenta komputera	
5	Możliwości monitora:	----------
A	Monitor musi posiadać możliwość montażu na ścianie z wykorzystaniem otworów montażowych w standardzie VESA 100	
B	Ekran o przekątnej 19 cali panoramiczny (16:10), WXGA+, TFT TN LED	
C	Rozdzielczość minimum 1440x900 pikseli	
D	Czas reakcji matrycy maksimum 5ms	
E	Kontrast minimum 1000:1 (typowy), 2000000:1 (dynamiczny)	
F	Ilość kolorów 16,7 mln	
G	Gniazda wejściowe: D-Sub 15pin, DVI-D, DisplayPort	
H	Pobór mocy monitora do 42W podczas pracy, do 0,5W podczas spoczynku	
I	Waga monitora do 2,6kg (ze względu na zachowanie wysokiego bezpieczeństwa podczas montażu na wysięgnikach)	
J	Monitor musi posiadać możliwość regulacji pochylenia, wysokości, cyfrowej (OSD), panel obrotowy (pivot), obrotową podstawę	
K	Monitor musi być wyposażony we wszystkie niezbędne kable przyłączeniowe m.in. kabel D-Sub, kabel DisplayPort, kabel zasilający	
L	Monitor musi posiadać wbudowany hub USB, możliwość zabezpieczenia Kensington, wbudowany zasilacz	
M	Monitor musi posiadać minimum certyfikaty: Energy Star 5,1 i EPEAT Gold	
6	Warunki gwarancji:	----------
A	Gwarancja 36 miesięcy od momentu podpisania protokołu odbioru	
B	Serwis musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta	Nazwa…… Siedziba……
C	Czas usunięcia uszkodzenia 7 dni roboczych od momentu pisemnego zgłoszenia awarii, sprzęt do naprawy i z naprawy Wykonawca dostarcza na swój koszt, w przypadku niemożności naprawy w w/w terminie - dostarczenie sprzętu zastępczego o nie gorszych parametrach technicznych	
D	Dostarczony sprzęt musi być fabrycznie nowy, nie starszy niż 6 miesięcy od daty produkcji	
Podać oferowany model: ……		

Minimalne wymagania dla systemu operacyjnego zainstalowanego na komputerach objętych niniejszym zamówieniem części nr 1

Lp.	Wymagania minimalne systemu operacyjnego	Czy spełnia ?
1	**2**	**3**
1	Wymagania dla systemu 64bit:	----------
A	Nie wymaga aktywacji za pomocą telefonu lub Internetu u producenta	
B	Dołączony nośnik z oprogramowaniem	

C	Licencja dożywotnia użytkownika	
D	Poprawna obsługa pamięci operacyjnej w ilości powyżej 4GB	
2	System musi spełniać następujące wymagania poprzez natywne dla niego mechanizmy, bez użycia dodatkowych aplikacji:	----------
A	możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat); internetowa aktualizacja zapewniona w języku polskim; wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IPv4 i IPv6; zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe; wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi); funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer; interfejs użytkownika działający w trybie graficznym z elementami 3D; zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta; możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników; zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych; zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych; funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego; funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika; zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi; wbudowany system pomocy w języku polskim; możliwość przystosowania stanowiska dla osób niepełnosprawnych (i słabo widzących);	
B	możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; wsparcie dla logowania przy pomocy smartcard; rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji; system posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; wsparcie dla Sun Java i .NET Framework 1.1, 2.0, 3.0 i 4.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach; wsparcie dla Jscript i VBScript – możliwość uruchamiania interpretera poleceń; zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem; rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami (obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową); rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację; graficzne środowisko instalacji i konfiguracji; transakcyjny system plików pozwalający na stosowanie przydziałów na	

	dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe; zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe; udostępnianie modemu; oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; możliwość przywracania plików systemowych; system operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.); możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (i przy użyciu numerów identyfikacyjnych sprzętu);	
3	Współpraca z posiadanymi aplikacjami:	----------
A	ze względu na posiadane przez Zamawiającego oprogramowanie Microsoft Office 2003/2007/2010/2013 wymagana jest możliwość instalacji tego oprogramowania na systemie operacyjnym oferowanym przez Wykonawcę	
B	ze względu na posiadaną przez Zamawiającego aplikację bazodanową InfoMedica (firmy Asseco Poland S.A.) wymagana jest możliwość instalacji tego oprogramowania na systemie operacyjnym oferowanym przez Wykonawcę. Dostarczone komputery będą wykorzystane do pracy z systemem AMMS (firmy Asseco Poland), który korzysta z przeglądarki internetowej, wtyczki Java, Wtyczki Flash.	
C	zaoferowany system operacyjny będzie mógł być wykorzystywany (bez konieczności wykonywania jakichkolwiek modyfikacji) w sieciach informatycznych do przetwarzania informacji wrażliwych (dane osobowe, dane medyczne, dane finansowe)	
4	Możliwość wykonania downgrad'u (zmiany wersji na niższą) w ramach posiadanej licencji (bez konieczności posiadania/dokupowania dodatkowej licencji na obniżaną wersję systemu)	
Podać nazwę, wersję oferowanego oprogramowania: …….		

* *wypełnia czytelnie 3 kolumnę Wykonawca*

Minimalne wymagania dla systemu pakietu bezpieczeństwa zainstalowanego na komputerach objętych niniejszym zamówieniem

***UWAGA**: Zamawiający obecnie posiada pakiet antywirusowy ESET Endpoint Security Suite (w sumie 341 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.

1. Oprogramowanie to będzie używane na dostarczonych stacjach roboczych
2. Udzielona licencja powinna umożliwić użytkowanie programu Zamawiającego będącego samodzielnym publicznym zakładem opieki zdrowotnej,
3. 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:*** • Pełne wsparcie dla systemu Windows Vista/Windows 7/Windows 8/8.1/Windows 10 • Wsparcie dla 32- i 64-bitowej wersji systemu Windows lub innego dostarczonego razem z komputerami • Wersja programu 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). • 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
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.

Podać nazwę, wersję oferowanego oprogramowania: ……

Oświadczam ,że oferowany przedmiot zamówienia spełnia wszystkie wymienione w powyższej tabeli wymagania

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

D/ZP/381/101B/15
Załącznik nr 5.1

FORMULARZ CENOWY
WYSZCZEGÓLNIENIE ASORTYMENTOWE I ILOŚCIOWE PRZEDMIOTU ZAMÓWIENIA
o parametrach jakościowych i technicznych wyszczególnionych w zał. nr 4.1
CZĘŚĆ 1- ZESTAWY KOMPUTEROWE

Lp.	Nazwa	J.m.	Ilość	Cena jednostkowa netto	Wartość netto	Podatek VAT	Wartość brutto
1	Zestaw komputerowy (komputer stacjonarny, monitor, system operacyjny, pakiet bezpieczeństwa)	komplet	15				

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

D/ZP/381/101B/15
Załącznik nr 4.2
.....
pieczęć firmowa wykonawcy

WYMAGANE i OFEROWANE PARAMETRY JAKOŚCIOWE i TECHNICZNE PRZEDMIOTU ZAMÓWIENIA
CZĘŚC 2 – KOMPUTERY PRZENOŚNE

Pozycja 1. KOMPUTER PRZENOŚNY TYPU ULTRABOOK – ILOŚĆ 1 SZTUKA

Lp.	*Wymagania minimalne*
1	Gwarancja 36 miesięcy na całe urządzenie od momentu podpisania protokołu odbioru
2	Serwis urządzenia musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta
3	Czas usunięcia uszkodzenia 14 dni roboczych od momentu pisemnego zgłoszenia awarii, sprzęt do naprawy i z naprawy Wykonawca dostarcza na swój koszt, w przypadku niemożności naprawy w w/w terminie - dostarczenie sprzętu zastępczego o nie gorszych parametrach techniczno-użytkowych
4	W przypadku awarii i konieczności zabrania komputera przenośnego z siedziby Zamawiającego pamięć masowa (dyski) pozostaje u Zamawiającego
5	W przypadku uszkodzenia pamięci masowej (dysku/ów) - uszkodzona pozostaje własnością Zamawiającego
6	Urządzenie musi być objęte ochroną przed przypadkowym uszkodzeniem;
7	Dostępność wszystkich sterowników koniecznych do prawidłowej pracy zestawu poprzez witrynę producenta zestawu komputerowego;
8	Komputer przenośny typu laptop (ultrabook);
9	Zastosowanie: praca sieciowa w aplikacji bazodanowej, praca z wykorzystaniem przeglądarki internetowej, praca z pakietem biurowym, praca z multimediami, całodniowa praca bez stałego źródła zasilania;
10	Wydajność obliczeniowa komputera na podstawie testów aplikacyjnych MobileMark2012 (www.bapco.com): w teście MobileMark 2012 Performance Rating minimum 127 pkt., Battery Life minimum 720 minut (12h);
11	Pamięć operacyjna: 4GB typu DDR3 w jednym slocie;
12	Możliwość rozbudowy do 8GB;
13	Interfejsy sieciowe wbudowane: WiFi 802.11b/g/n, Bluetooth;
14	Karta graficzna pracująca w trybie Full HD z pamięcią dynamiczną;
15	Ekran o przekątnej 13,3 cali, matryca HD, z powłoką antyrefleksyjną, odporny na zarysowania;
16	Obudowa ze zwiększoną odpornością np. z wykorzystaniem aluminium / włókien węglowych;
17	Rozdzielczość nominalna 1920x1080 pikseli;
18	Pamięć masowa minimum 128GB SSD (flash) SATA III;
19	Zintegrowana karta dźwiękowa i mikrofon, głośniki stereo, kamera internetowa;
20	Klawiatura pełnowymiarowa, panel dotykowy z obsługą gestów;
21	Wyjścia video: mini DisplayPort (należy dołączyć kabel z przejściem z mini DisplayPort na HDMI);
22	Zgodność z systemami operacyjnymi i standardami potwierdzona certyfikatem WHCL oraz certyfikatem CE;
23	Certyfikat EnergyStar 6.0;
24	Złącza zewnętrzne: słuchawkowe 1 sztuka, USB 3.0 2 sztuki;
25	Możliwość odczytania z BIOS: (wersji BIOS, modelu procesora wraz z informacjami o ilości rdzeni, prędkościach min i max zegara, wielkości podręcznej pamięci Cache, informacji o ilości pamięci RAM, informacji o dysku twardym);
26	Możliwość wyłączenia zintegrowanej(nych) karty sieciowej, możliwość wyłączenia portów USB z poziomu BIOS bez uruchamiania systemu operacyjnego komputera;
27	Funkcja blokowania/odblokowywania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego;
28	Możliwość ustawienia hasła na poziomie administratora bez potrzeby uruchamiania systemu operacyjnego;
29	Nie dopuszcza się stosowania tzw. overclockingu w celu uzyskania wymaganych parametrów pracy zestawu komputerowego;
30	Zainstalowany system operacyjny w wersji do zastosowań businessowych, profesjonalnych wg wymagań wyszczególnionych w dalszej części siwz wraz z nośnikiem instalacyjnym na płycie DVD i

	licencją dożywotnią;
31	Zainstalowany pakiet antywirusowy w wersji do zastosowań komercyjnych, profesjonalnych wg wymagań wyszczególnionych w dalszej części siwz
32	Zainstalowany pakiet biurowy w wersji do zastosowań komercyjnych, profesjonalnych wg wymagań wyszczególnionych w dalszej części siwz
33	Waga do 1,4 kg (z baterią);
34	Akcesoria dodatkowe: bezprzewodowa mysz optyczna (z gwarancją minimum 2 lata, dla prawo i lewo ręcznych, 3 przyciski, rolka do przewijania, z nano odbiornikiem do komunikacja z laptopem); torba przenośna na laptop o wymiarze dopasowanym do laptopa z minimum jedną dodatkową kieszenią na zasilacz i inne akcesoria np. myszkę; karta sieciowa podłączana do laptopa przez port USB o prędkości 100/1000Mbps i złączu kablowym RJ45;
35	Urządzenie fabrycznie nowe;
Podać oferowany model:	……

Pozycja 2. KOMPUTER PRZENOŚNY TYPU LAPTOP – ILOŚĆ 1 SZTUKA

Lp.	*Wymagania minimalne*
1	Gwarancja 24 miesiące na całe urządzenie od momentu podpisania protokołu odbioru
2	Serwis urządzenia musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta
3	Czas usunięcia uszkodzenia 14 dni roboczych od momentu pisemnego zgłoszenia awarii, sprzęt do naprawy i z naprawy Wykonawca dostarcza na swój koszt, w przypadku niemożności naprawy w w/w terminie - dostarczenie sprzętu zastępczego o nie gorszych parametrach techniczno-użytkowych
4	W przypadku awarii i konieczności zabrania komputera przenośnego z siedziby Zamawiającego pamięć masowa (dyski) pozostaje u Zamawiającego
5	W przypadku uszkodzenia pamięci masowej (dysku/ów) - uszkodzona pozostaje własnością Zamawiającego
6	Urządzenie musi być objęte ochroną przed przypadkowym uszkodzeniem;
7	Dostępność wszystkich sterowników koniecznych do prawidłowej pracy zestawu poprzez witrynę producenta zestawu komputerowego;
8	Komputer przenośny typu laptop;
9	Zastosowanie: praca sieciowa w aplikacji bazodanowej, praca z wykorzystaniem przeglądarki internetowej, praca z pakietem biurowym, praca z multimediami, całodniowa praca bez stałego źródła zasilania;
10	Wydajność obliczeniowa komputera na podstawie testów aplikacyjnych MobileMark2014 (www.bapco.com): w teście MobileMark 2014 Performance Rating minimum 1500 pkt., Battery Life minimum 600 minut (10h);
11	Pamięć operacyjna: 8GB typu DDR3;
12	Napęd optyczny DVD+/-RW
13	Interfejsy sieciowe wbudowane: WiFi 802.11b/g/n, Bluetooth 4.0; 100/1000Mbps RJ45;
14	Karta graficzna pracująca w trybie Full HD z własną pamięcią;
15	Ekran o przekątnej 17,3 cali, matryca HD+, błyszcząca;
16	Czytnik kart pamięci (SD,SDHC,SDXC)
17	Rozdzielczość nominalna 1600x900 pikseli;
18	Pamięć masowa minimum 1TB HDD SATA III;
19	Zintegrowana karta dźwiękowa i mikrofon, głośniki stereo, kamera internetowa;
20	Klawiatura pełnowymiarowa z wydzieloną klawiaturą numeryczną, panel dotykowy;
21	Wyjścia video: 1 HDMI
22	Zgodność z systemami operacyjnymi i standardami potwierdzona certyfikatem WHCL oraz certyfikatem CE;
23	Certyfikat EnergyStar;
24	Złącza zewnętrzne: słuchawkowe 1 sztuka, USB3.0 1 sztuka USB2.0 2 sztuki;
25	Możliwość odczytania z BIOS: (wersji BIOS, modelu procesora wraz z informacjami o ilości rdzeni, prędkościach min i max zegara, wielkości podręcznej pamięci Cache, informacji o ilości pamięci RAM, informacji o dysku twardym);
26	Możliwość wyłączenia zintegrowanej(nych) karty sieciowej, możliwość wyłączenia portów USB z

	poziomu BIOS bez uruchamiania systemu operacyjnego komputera;
27	Funkcja blokowania/odblokowywania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego;
28	Możliwość ustawienia hasła na poziomie administratora bez potrzeby uruchamiania systemu operacyjnego;
29	Nie dopuszcza się stosowania tzw. overclockingu w celu uzyskania wymaganych parametrów pracy zestawu komputerowego;
30	Zainstalowany system operacyjny w wersji do zastosowań businessowych, profesjonalnych wg wymagań wyszczególnionych w dalszej części siwz wraz z nośnikiem instalacyjnym na płycie DVD i licencją dożywotnią;
31	Zainstalowany pakiet antywirusowy w wersji do zastosowań komercyjnych, profesjonalnych wg wymagań wyszczególnionych w dalszej części siwz
32	Waga do 3,0 kg (z baterią);
33	Akcesoria dodatkowe: bezprzewodowa mysz optyczna (z gwarancją minimum 2 lata, dla prawo i lewo ręcznych, 3 przyciski, rolka do przewijania, z nano odbiornikiem do komunikacja z laptopem); torba przenośna na laptop o wymiarze dopasowanym do laptopa z minimum jedną dodatkową kieszenią na zasilacz i inne akcesoria np. myszkę;
34	Urządzenie fabrycznie nowe;
Podać oferowany model	

MINIMALNE WYMAGANIA DLA SYSTEMU OPERACYJNEGO ZAINSTALOWANEGO NA KOMPUTERACH OBJĘTYCH NINIEJSZYM ZAMÓWIENIEM część 2

Lp.	Wymagania minimalne systemu operacyjnego
1	Wymagania dla systemu 64bit:
A	Nie wymaga aktywacji za pomocą telefonu lub Internetu u producenta
B	Dołączony nośnik z oprogramowaniem
C	Licencja dożywotnia użytkownika
D	Poprawna obsługa pamięci operacyjnej w ilości powyżej 4GB
2	System musi spełniać następujące wymagania poprzez natywne dla niego mechanizmy, bez użycia dodatkowych aplikacji:
A	możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat); internetowa aktualizacja zapewniona w języku polskim; wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IPv4 i IPv6; zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe; wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi); funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer; interfejs użytkownika działający w trybie graficznym z elementami 3D; zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta; możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników; zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych; zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych; funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego; funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika; zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi; wbudowany system pomocy w języku polskim; możliwość przystosowania stanowiska dla osób niepełnosprawnych (i słabo widzących);

B	możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; wsparcie dla logowania przy pomocy smartcard; rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji; system posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; wsparcie dla Sun Java i .NET Framework 1.1, 2.0, 3.0 i 4.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach; wsparcie dla Jscript i VBScript – możliwość uruchamiania interpretera poleceń; zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem; rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami (obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową); rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację; graficzne środowisko instalacji i konfiguracji; transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe; zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe; udostępnianie modemu; oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; możliwość przywracania plików systemowych; system operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.); możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (i przy użyciu numerów identyfikacyjnych sprzętu);
3	Współpraca z posiadanymi aplikacjami:
A	ze względu na posiadane przez Zamawiającego oprogramowanie Microsoft Office 2003/2007/2010/2013 wymagana jest możliwość instalacji tego oprogramowania na systemie operacyjnym oferowanym przez Wykonawcę
B	ze względu na posiadaną przez Zamawiającego aplikację bazodanową InfoMedica (firmy Asseco Poland S.A.) wymagana jest możliwość instalacji tego oprogramowania na systemie operacyjnym oferowanym przez Wykonawcę Dodatkowo na dostarczonych komputerach musi być możliwość uruchomienia systemu AMMS (firmy Asseco Poland) który korzysta z przeglądarki internetowej, wtyczki Java, Wtyczki Flash
C	zaoferowany system operacyjny będzie mógł być wykorzystywany (bez konieczności wykonywania jakichkolwiek modyfikacji) w sieciach informatycznych do przetwarzania informacji wrażliwych (dane osobowe, dane medyczne, dane finansowe)
4	Możliwość wykonania downgrad'u (zmiany wersji na niższą) w ramach posiadanej licencji (bez konieczności posiadania dodatkowej licencji na obniżaną wersję systemu)
Podać nazwę, wersję oferowanego oprogramowania: …….	

MINIMALNE WYMAGANIA DLA PAKIETU BIUROWEGO ZAINSTALOWANEGO NA KOMPUTERZE PRZENOŚNYM TYPU ULTRABOOK

Lp.	Wymagania minimalne pakietu biurowego
1	Pakiet zintegrowanych aplikacji biurowych musi zawierać:
A	Edytor tekstu
B	Arkusz kalkulacyjny
C	Narzędzie do przygotowywania i prowadzenia prezentacji
D	Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
E	Narzędzie do tworzenia notatek
2	Pakiet biurowy musi spełniać następujące wymagania:
2.1	Wymagania odnośnie interfejsu użytkownika:
A	pełna polska wersja językowa interfejsu użytkownika z możliwością, przełączania wersji językowej interfejsu na język angielski; prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych; możliwość zintegrowania uwierzytelniania użytkowników z

	usługą katalogową (Active Direktory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się; oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców; w skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy); do aplikacji musi być dostępna pełna dokumentacja w języku polskim;
B	oprogramowanie musi umożliwiać tworzenie i edycję dokumentów, elektronicznych w ustalonym formacie, który spełnia następujące warunki: posiada kompletny i publicznie dostępny opis formatu; ma zdefiniowany układ informacji w postaci XML; umożliwia wykorzystanie schematów XML; wspiera w swojej specyfikacji podpis elektroniczny;
2.2	Edytor tekstów musi umożliwiać:
A	edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty; wstawianie oraz formatowanie tabel; wstawianie oraz formatowanie obiektów graficznych; wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne); automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków; automatyczne tworzenie spisów treści; formatowanie nagłówków i stopek stron; sprawdzanie pisowni w języku polskim; śledzenie zmian wprowadzonych przez użytkowników; nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności; określenie układu strony (pionowa/pozioma); wydruk dokumentów; wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną; pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003/2007 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu; zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji; wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem; wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa;
2.3	Arkusz kalkulacyjny musi umożliwiać:
A	tworzenie raportów tabelarycznych; tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych; tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu; tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice); obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych; narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych; tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych; wyszukiwanie i zamianę danych; wykonywanie analiz danych przy użyciu formatowania warunkowego; nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie; nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności; formatowanie czasu, daty i wartości finansowych z polskim formatem; zapis wielu arkuszy kalkulacyjnych w jednym pliku; zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003/2007/2010 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń; zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji;
2.4	Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
A	prezentowanie przy użyciu projektora multimedialnego; drukowanie w formacie umożliwiającym robienie notatek; zapisanie jako prezentacja tylko do odczytu; nagrywanie narracji i dołączanie jej do prezentacji; opatrywanie slajdów notatkami dla prezentera; umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo; umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego; odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym; możliwość tworzenia animacji obiektów i całych slajdów; prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera; pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003/2007/2010;
2.5	Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i

	zadaniami) musi umożliwiać:
A	pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego; filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców; tworzenie katalogów, pozwalających katalogować pocztę elektroniczną; automatyczne grupowanie poczty o tym samym tytule; tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy; oflagowanie poczty elektronicznej z określeniem terminu przypomnienia; zarządzanie kalendarzem; udostępnianie kalendarza innym użytkownikom; przeglądanie kalendarza innych użytkowników; zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach; zarządzanie listą zadań; zlecanie zadań innym użytkownikom; zarządzanie listą kontaktów; udostępnianie listy kontaktów innym użytkownikom; przeglądanie listy kontaktów innych użytkowników; możliwość przesyłania kontaktów innym użytkowników;
3	Udzielona licencja musi umożliwić użytkowanie oprogramowania do celów komercyjnych przez 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. **Licencja na zaproponowane oprogramowanie zezwala na przenoszenie (przeinstalowywanie) oprogramowania pomiędzy komputerami dowolną ilość razy bez ograniczeń, jest w formie pudełkowej, nośnik w formie dowolnej tj. płyta dvd/plik do pobrania z internetu, wieczysta, wersja językowa polska.**
Podać nazwę, wersję oferowanego oprogramowania: ……..	

MINIMALNE WYMAGANIA DLA SYSTEMU PAKIETU BEZPIECZEŃSTWA ZAINSTALOWANEGO NA KOMPUTERACH OBJĘTYCH NINIEJSZYM ZAMÓWIENIEM – CZĘŚĆ 2

***UWAGA**: Zamawiający obecnie posiada pakiet antywirusowy ESET Endpoint Security Suite (w sumie 341 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.

1. Oprogramowanie to będzie używane na dostarczonych komputerach przenośnych
2. Udzielona licencja powinna umożliwić użytkowanie programu Zamawiającego będącego samodzielnym publicznym zakładem opieki zdrowotnej,
3. 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 laptopów:*** • Pełne wsparcie dla systemu Windows Vista/Windows 7/Windows 8/8.1/Windows 10 • Wsparcie dla 32- i 64-bitowej wersji systemu Windows lub innego dostarczonego razem z komputerami • 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). • 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
Podać nazwę, wersję oferowanego oprogramowania:	

Oświadczam ,że oferowany przedmiot zamówienia spełnia wszystkie wymienione w powyższej tabeli wymagania

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

D/ZP/381/101B/15
Załącznik nr 5.2

FORMULARZ CENOWY
WYSZCZEGÓLNIENIE ASORTYMENTOWE I ILOŚCIOWE PRZEDMIOTU ZAMÓWIENIA
o parametrach jakościowych i technicznych wyszczególnionych w zał. nr 4.2
CZĘŚĆ 2 - KOMPUTERY PRZENOŚNE

Lp.	Nazwa	J.m.	Ilość	Cena jednostkowa netto	Wartość netto	Podatek VAT	Wartość brutto
1	Komputer przenośny ultrabook (komputer przenośny ultrabook, system operacyjny, pakiet bezpieczeństwa,pakiet biurowy)	Sztuk	1				
2	Komputer przenośny typu laptop (Komputer przenośny typu laptop system operacyjny, pakiet bezpieczeństwa)	Sztuk	1				
RAZEM:							

.....

podpis i pieczęć osoby uprawnionej/osób uprawnionych

do reprezentowania wykonawcy

D/ZP/381/101B/15
Załącznik nr 4.3
.....
pieczęć firmowa wykonawcy

WYMAGANE i OFEROWANE PARAMETRY JAKOŚCIOWE i TECHNICZNE PRZEDMIOTU ZAMÓWIENIA
CZĘŚC 3 – CZYTNIKI KART CHIPOWYCH
(ilość 5 sztuk)

Lp.	*Wymagania minimalne*
1	Czytnik odczytujący karty chipowe z Narodowego Funduszu Zdrowia
2	Zasilacz ,przewody niezbędne do podłączenia czytnika do komputera przez port USB
3	Czytnik musi współpracować z oprogramowaniem posiadanym przez Zamawiającego InfoMedica/AMMS firmy ASSECO POLAND
	Warunki gwarancji:
1	Minimum 24 miesiące na urządzenie od dnia podpisania protokołu odbioru
2	Czas usunięcia uszkodzenia 7 dni roboczych od momentu pisemnego zgłoszenia awarii, sprzęt do naprawy i z naprawy Wykonawca dostarcza na swój koszt, w przypadku niemożności naprawy w w/w terminie – dostarczenie sprzętu zastępczego o nie gorszych parametrach techniczno-użytkowych
3	Serwis urządzenia musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta
Marka ,model , producent oferowanych czytników ……	

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

D/ZP/381/101B/15
Załącznik nr 5.3

FORMULARZ CENOWY
WYSZCZEGÓLNIENIE ASORTYMENTOWE I ILOŚCIOWE PRZEDMIOTU ZAMÓWIENIA
o parametrach jakościowych i technicznych wyszczególnionych w zał. nr 4.3
Część 3–CZYTNIK KART CHIPOWYCH

Lp.	Nazwa	J.m.	Ilość	Cena jednostkowa netto	Wartość netto	Podatek VAT	Wartość brutto
1	Czytnik kart chipowych	Sztuk	5				

.....

podpis i pieczęć osoby uprawnionej/osób uprawnionych
do reprezentowania wykonawcy

D/ZP/381/101B/15
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. .....

.....
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/381/101B/15
Załącznik nr 7

UMOWA – wzór

Zawarta w dniu ..... w Katowicach pomiędzy:

Uniwersyteckie 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

a

.....…
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

Na podstawie oferty wybranej w/w postępowaniu Zamawiający zamawia, a Wykonawca przyjmuje do wykonania sprzedaż, dostarczenie sprzętu komputerowego w ilości i asortymencie określonym w załączniku nr 1 do umowy, którego parametry jakościowe i techniczne określone zostały w załączniku nr 4.1 do 4.3 Specyfikacji Istotnych Warunków Zamówienia.

§ 2.
WARUNKI REALIZACJI UMOWY

1. Wykonawca zobowiązuje się do zrealizowania umowy zgodnie z warunkami określonymi w Specyfikacji Istotnych Warunków Zamówienia.
2. Wykonawca oświadcza i gwarantuje, że dostarczony sprzęt komputerowy jest fabrycznie nowy, nie starszy niż 6 miesięcy od daty produkcji, pochodzi z oficjalnego kanału sprzedaży producenta na rynek polski i posiada wszystkie wymagane prawem certyfikaty lub dokumenty równoważne,
3. Wykonawca zobowiązuje się dostarczyć sprzęt komputerowy w terminie do ……*(zgodnie z zaoferowanym w ofercie terminem dostawy)* dni kalendarzowych od dnia zawarcia umowy. Wykonanie obowiązków Wykonawcy określonych w niniejszej umowie zostanie potwierdzone Protokołem Odbioru podpisanym przez obie Strony.
4. Wykonawca ponosi koszty transportu, rozładunku oraz ubezpieczenia sprzętu komputerowego do miejsca odbioru w siedzibie Zamawiającego.
5. Miejscem odbioru sprzętu komputerowego jest Dział Informatyki znajdujący się w siedzibie Zamawiającego.

§ 3.
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. Ceny jednostkowe sprzętu komputerowego określone zostały w załączniku nr 1 do umowy.
3. Zamawiający zapłaci Wykonawcy wynagrodzenie o którym mowa w ust.1 w ciągu 30 dni od otrzymania faktury VAT wystawionej po podpisaniu Protokołu Odbioru. W przypadku gdyby Wykonawca zamieścił na fakturze inny termin płatności niż określony w niniejszej umowie obowiązuje termin płatności określony w umowie.
4. Za datę zapłaty przyjmuje się datę obciążenia rachunku bankowego Zamawiającego.

§ 4.

GWARANCJA, REALIZACJA UPRAWNIEŃ GWARANCYJNYCH

1. Wykonawca udziela gwarancji na oferowany sprzęt komputerowy zgodnie z zasadami określonymi w załączniku nr 4.1 do 4.3 SIWZ. Okres gwarancji rozpoczyna bieg od dnia odbioru sprzętu potwierdzonego Protokołem Odbioru, o którym mowa w § 2.ust 3 umowy.
2. Odpowiedzialność z tytułu gwarancji obejmuje wszelkie wady sprzętu komputerowego nie wynikające z winy Zamawiającego. W okresie gwarancji Wykonawca jest zobowiązany nieodpłatnie dokonać naprawy lub wymiany sprzętu lub jego poszczególnych części - także w przypadku, gdy konieczność naprawy lub wymiany jest wynikiem eksploatacyjnego zużycia sprzętu lub jego części.
3. Wykonawca gwarantuje naprawę uszkodzonego sprzętu komputerowego albo wymianę sprzętu lub jego części na nowe w terminie liczonym od zgłoszenia awarii nie dłuższym niż 7 dni roboczych *(część 1)* i 14 dni roboczych *(część 2 i 3)*
4. Obsługa serwisowa gwarancyjna będzie prowadzona przez autoryzowany serwis techniczny ..... z siedzibą ..... O zmianie podmiotu świadczącego usługi serwisowe Wykonawca niezwłocznie powiadomi Zamawiającego na piśmie.
5. Zgłoszenia awarii dokonywane będą za pośrednictwem poczty elektronicznej na adres e-mail: ..... lub za pośrednictwem faxu na numer……
6. W przypadku naprawy sprzętu komputerowego trwającej dłużej niż określono w ust.3 , Wykonawca zobowiązany jest nieodpłatnie dostarczyć na okres przedłużającej się naprawy sprawne urządzenie zastępujące w pełni urządzenie naprawiane.
7. W przypadku, gdy liczba napraw gwarancyjnych przekroczy 3 naprawy tego samego urządzenia lub podzespołu Wykonawca zobowiązany jest do wymiany urządzenia lub podzespołu na nowe (z wyjątkiem uszkodzeń z winy użytkownika).Wymiana urządzenia lub podzespołu nastąpi w terminie określonym w ust.3.
8. W przypadku awarii i konieczności zabrania sprzętu komputerowego z siedziby Zamawiającego jak również w przypadku konieczności wymiany uszkodzonej pamięci masowej (dysków) w ramach naprawy gwarancyjnej dysk twardy podlegający wymianie pozostaje własnością Zamawiającego.
10. Wszelkie koszty związane z usunięciem awarii objętych gwarancją w tym koszty transportu sprzętu do naprawy i z naprawy obciążają Wykonawcę.
11. Okres gwarancji udzielonej przez Wykonawcę ulega przedłużeniu o pełen okres niesprawności dostarczonego urządzenia.

§ 5.

KARY UMOWNE

1. Wykonawca zapłaci Zamawiającemu kary umowne:

a) za każdy dzień opóźnienia w realizacji obowiązków określonych w § 2 ust. 3 umowy - w wysokości 50,00 zł (słownie : pięćdziesiąt złotych);

b) za każdy dzień opóźnienia w wykonaniu naprawy gwarancyjnej względem terminu, o którym mowa w § 4 ust. 3 umowy – w wysokości 50,00zł (słownie: pięćdziesiąt złotych) o ile nie zostanie dostarczone tożsame urządzenie na czas przedłużającej się naprawy zgodnie z § 4 ust. 5 umowy,

c) w wysokości 10% kwoty wynagrodzenia brutto za daną część zamówienia określonego w §3 ust. 1 niniejszej umowy – w przypadku odstąpienia w tej części od umowy lub rozwiązania w tej części 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, aż do całkowitego zaspokojenia roszczeń. W przypadku braku możliwości zaspokojenia roszczeń z tytułu kar umownych na zasadach określonych powyżej, księgowa nota obciążeniowa płatna będzie do 14 dni od daty jej wystawienia przez Zamawiającego.
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 zaistnienia 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 powzięcia wiadomości o powyższych okolicznościach. W takim wypadku Wykonawca ma prawo żądać jedynie wynagrodzenia należnego z tytułu wykonania części umowy.
2. Zamawiający może rozwiązać umowę w zakresie danej części określonej w §3 ust 1 ze skutkiem natychmiastowym w przypadku gdy opóźnienie w realizacji obowiązków określonych w § 2 ust. 3 przekroczy 10 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. W sprawach nieuregulowanych niniejszą umową mają zastosowanie odpowiednie przepisy ustawy - Prawo zamówień publicznych i Kodeksu cywilnego.
2. W przypadku niejasności w zapisach niniejszej umowy Strony mogą odwołać się do zapisów w Specyfikacji Istotnych Warunków Zamówienia.
3. 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.
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 wyrażeniu zgody przez podmiot tworzący Zamawiającego.
5. Wszelkie spory wynikłe na tle realizacji umowy będzie rozstrzygał sąd powszechny właściwy dla siedziby Zamawiającego.
6. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, dwa egzemplarze dla Zamawiającego, jeden egzemplarz dla Wykonawcy.

Załączniki do umowy:

1 - Wyszczególnienie asortymentowe , ilościowe, ceny jednostkowe przedmiotu umowy.

Wykonawca **Zamawiający**