KOPERNIK

Łódź, dnia 06.09.2015 r
Nr sprawy 155/ZP/15

Zamawiający:
WOJEWÓDZKI SZPITAL SPECJALISTYCZNY
im. M. Kopernika w Łodzi
ul. Pabianicka 62
93-513 Łódź
tel. (42) 689 58 19, 689 59 11
fax. (042) 689 54 09
www.kopernik.lodz.pl

Specyfikacja Istotnych Warunków Zamówienia (SIWZ)

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego o wartości powyżej 30 000 euro, nie przekraczającej 207 000 euro na **dostawę systemu informatycznego w oparciu o bezpieczeństwo sieciowe i usługi medyczne** dla Wojewódzkiego Szpitala Specjalistycznego im. M. Kopernika w Łodzi.

Liczba stron specyfikacji: 75

Zatwierdził:
Wojewódzkiego Szpitala Specjalistycznego
im. M. Kopernika w Łodzi
mgr Wojciech Szrajber

Ilekroć w niniejszej SIWZ jest mowa o „Ustawie" należy przez to rozumieć Ustawę z dnia 29 stycznia 2004 r. Prawo Zamówień Publicznych (Dz. U. z 2013 r. poz. 907 tekst jednolity z późn. zm.).

I. PRZEDMIOT ZAMÓWIENIA

1. Przedmiotem zamówienia jest **dostawa systemu informatycznego** wyszczególnionych ilościowo i asortymentowo oraz opisanych w **załączniku nr 1 do SIWZ.**

Lp.	Przedmiot	Ilość
1.	System zabezpieczenia sieci w punkcie styku z internetem pracujący w trybie redundancji	2 systemy
2.	Przełączniki rdzeniowe	2 sztuki
3.	Rozbudowa obudowy HP Blade System C3000:	
3.1	Moduły LAN	4 sztuki
3.2	Karty Ethernet	6 sztuk
3.3	Moduły SAN	2 sztuki
4.	System kopii zapasowych	1 system
5.	System Obsługi Zakładu diagnostyki Obrazowej (RIS)	1 system
6.	Licencja na oprogramowanie przeglądarki medycznej obrazów DICOM	1 licencja
7.	System antywirusowy dla stacji klienckich i serwerów	1060 licencji
8.	Usługi wdrożeniowe do 31.12.2015r.	1 usługa
9.	Wsparcie utrzymaniowe	12 miesięcy – po zakończeniu usługi wdrożeniowej

2. Przedmiot zamówienia określony jest we **Wspólnym Słowniku Zamówień** pod kodem i pojęciem:

Kod CPV	Opis
30236000-2	**Różny sprzęt komputerowy**

3. Przedmiot zamówienia nie został podzielony na pakiety.

4. Oferta **musi o**bejmować całość zamówienia.

5. Zamawiający wymaga, by oferowane towary spełniały wymogi określone obowiązującym prawem, zostały dopuszczone do obrotu handlowego i posiadały wymagane prawem ważne dokumenty, stwierdzające dopuszczenie do stosowania na terenie Polski.

6. Zamawiający nie dopuszcza składania ofert wariantowych zgodnie z art. 83 ust. 1 ustawy PZP.

7. Zamawiający nie przewiduje aukcji elektronicznej w niniejszym postępowaniu.

8. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

9. Zamawiający dopuszcza udział podwykonawców w realizacji niniejszego zamówienia. W przypadku, gdy Wykonawca przewiduje wykonanie zamówienia z udziałem podwykonawców należy wskazać w

treści oferty która część (części) zamówienia powierzona zostanie podwykonawcy (podwykonawcom) wraz z wykazem zakresu zadań zlecanych Podwykonawcom, a w przypadku, gdy Wykonawca powołuje się, na zasadach określonych w art. 26 ust. 2b ustawy Pzp, w celu wykazania spełniania warunków udziału w postępowaniu, o których mowa w art. 22 ust. 1 ustawy Pzp, na zasoby takiego podwykonawcy, zobowiązany jest podać nazwę (firmę) takiego podwykonawcy. W przypadku nie złożenia stosownego oświadczenia Zamawiający uzna, iż Wykonawca zamierza wykonać zadanie samodzielnie.

10. Zamawiający nie przewiduje zamówień uzupełniających w ramach niniejszego postępowania.

II. WARUNKI REALIZACJI ZAMÓWIENIA

1. Umowa zostanie zawarta na okres 18 miesięcy. W pierwszej kolejności zrealizowana zostanie dostawa sprzętu i oprogramowania wraz z licencjami. Jednocześnie od dnia zawarcia umowy do 31.12.2015r. zrealizowana zostanie usługa wdrożeniowa. Następnie przez okres 12 miesięcy świadczona będzie usługa wsparcia utrzymaniowego.

2. Realizacja przyszłej umowy będzie nadzorowana przez **Dział Informatyki.**

3. Miejsce realizacji dostawy i usług: WSS im. M. Kopernika w Łodzi – Łódź, ul. Pabianicka 62.

4. Płatność za zrealizowaną dostawę oraz usługi wdrożeniowe będzie następowała w 12 równych miesięcznych ratach. Płatność za usługi wsparcia utrzymaniowego również będzie następowała w 12 równych ratach i rozpocznie się po zakończeniu usługi wdrożeniowej. Termin płatności wynosi 60 dni od dnia dostarczenia prawidłowo wystawionej faktury VAT do siedziby Zamawiającego.

III. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

1. Wykonawca przedstawia ofertę zgodnie z wymogami określonymi w ustawie Prawo Zamówień Publicznych z dnia 29.01.2004 r. (Dz. U. z 2013 r. poz. 907 tekst jednolity z późn. zm.) oraz niniejszej Specyfikacji Istotnych Warunków Zamówienia (SIWZ).

2. Wykonawcy ponoszą wszelkie koszty związane z przygotowaniem i złożeniem oferty.

3. Jeden Wykonawca może złożyć tylko jedną ofertę. Złożenie większej liczby ofert spowoduje odrzucenie wszystkich ofert złożonych przez Wykonawcę.

4. Jeżeli oferta zawiera dokumenty, które stanowią tajemnicę przedsiębiorstw w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, składający ofertę zobowiązany jest do umieszczenia ich jako ostatnie stronice oferty oraz poprzedzenia oświadczeniem o zakazie udostępniania odpowiednich oznaczonych numerycznie stron.

5. Nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli wykonawca, nie później niż w terminie składania ofert lub wniosków o dopuszczenie do udziału w postępowaniu, zastrzegł, że nie mogą być one udostępniane **oraz wykazał,** iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, o których mowa w art. 86 ust. 4.

6. Oferta powinna być napisana w języku polskim (zgodnie z art. 9 ust. 2 Ustawy), na maszynie lub komputerze albo czytelnym pismem ręcznym oraz podpisana przez osobę upoważnioną do

reprezentowania Wykonawcy. Dokumenty złożone w językach obcych powinny być przetłumaczone, a kserokopia tłumaczenia oraz kserokopia oryginału dokumentu przetłumaczonego (potwierdzone za zgodność z oryginałem) stanowić będą załączniki do oferty.

7. Upoważnienie do podpisania oferty (w oryginale lub poświadczone przez notariusza) powinno być do niej dołączone, o ile nie wynika z innych dokumentów załączonych przez Wykonawcę.

8. Ofertę w jednym egzemplarzu wraz ze wszystkimi załącznikami na ponumerowanych kartkach zawierających informacje należy umieścić w kopercie, która będzie zaadresowana do Zamawiającego i opatrzona danymi Wykonawcy oraz napisem :

Przetarg nieograniczony na dostawę systemu informatycznego w oparciu o bezpieczeństwo sieciowe i usługi medyczne dla Wojewódzkiego Szpitala Specjalistycznego im. M. Kopernika w Łodzi
Znak sprawy – 155/ZP/15
Ilość stron _____
Nie otwierać przed dniem .....2015 r.

9. Dla uzyskania ważności oferta musi zawierać wszystkie wymagane oświadczenia i dokumenty wymienione w pkt. V SIWZ. Dokumenty muszą być w formie oryginału lub poświadczonej za zgodność z oryginałem kserokopii. Poświadczenie musi być dokonane przez Wykonawcę tj. osobę upoważnioną do jego reprezentacji.

Forma: własnoręczny podpis (jeśli jest to z pieczątką), data i napis „za zgodność z oryginałem".

10. Wszelkie zmiany lub poprawki w tekście oferty muszą być parafowane i datowane przez osobę podpisującą ofertę.

IV. WARUNKI UDZIAŁU W POSTĘPOWANIU, ORAZ OPIS SPOSOBU DOKONYWANIA OCENY SPEŁNIANIA TYCH WARUNKÓW

A. WARUNKI UDZIAŁU W POSTĘPOWANIU

1. O udzielenie zamówienia mogą ubiegać się wykonawcy, który **spełniają warunki, o których mowa w art. 22 ust. 1** ustawy Prawo zamówień publicznych tj.:
   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.

Wykonawca może polegać na wiedzy i doświadczeniu, potencjale technicznym, osobach zdolnych do wykonania zamówienia lub zdolnościach finansowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków. Wykonawca w takiej sytuacji zobowiązany jest udowodnić Zamawiającemu, iż będzie dysponował zasobami niezbędnymi do realizacji zamówienia, w szczególności przedstawiając w tym celu pisemne zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby wykonania zamówienia.

Podmiot, który zobowiązał się do udostępnienia zasobów zgodnie z ust. 2b, odpowiada solidarnie z wykonawcą za szkodę zamawiającego powstałą wskutek nieudostępnienia tych zasobów, chyba że za nieudostępnienie zasobów nie ponosi winy.

2. O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy **nie podlegają wykluczeniu z postępowania na podstawie art. 24 ust. 1 i 2** ustawy Prawo zamówień publicznych tj.:

   Z postępowania o udzielenie zamówienia wyklucza się:
   1) Wykonawców, w stosunku do których otwarto likwidację lub których upadłość ogłoszono, z wyjątkiem wykonawców, którzy po ogłoszeniu upadłości zawarli układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli poprzez likwidację majątku upadłego;
   2) Wykonawców, którzy zalegają z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, z wyjątkiem przypadków gdy uzyskali oni przewidziane prawem zwolnienie, odroczenie, rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu;
   3) osoby fizyczne, które prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przeciwko środowisku, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego;
   4) spółki jawne, których wspólnika prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przeciwko środowisku, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego;

5) spółki partnerskie, których partnera lub członka zarządu prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przeciwko środowisku, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego;
6) spółki komandytowe oraz spółki komandytowo-akcyjne, których komplementariusza prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przeciwko środowisku, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego;
7) osoby prawne, których urzędującego członka organu zarządzającego prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przeciwko środowisku, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego;
8) podmioty zbiorowe, wobec których sąd orzekł zakaz ubiegania się o zamówienia, na podstawie przepisów o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary;
9) Wykonawców będących osobami fizycznymi, które prawomocnie skazano za przestępstwo, o którym mowa w art. 9 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769) – przez okres 1 roku od dnia uprawomocnienia się wyroku;
10) Wykonawców będących spółką jawną, spółką partnerską, spółką komandytową, spółka komandytowo-akcyjną lub osobą prawną, których odpowiednio wspólnika, partnera, członka zarządu, komplementariusza lub urzędującego członka organu zarządzającego prawomocnie skazano za przestępstwo, o którym mowa w art. 9 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej – przez okres 1 roku od dnia uprawomocnienia się wyroku.
11) Wykonawców, którzy wykonywali bezpośrednio czynności związane z przygotowaniem prowadzonego postępowania, z wyłączeniem czynności wykonywanych podczas dialogu technicznego, o których mowa w art. 31a ust. 1 lub posługiwali się w celu sporządzenia oferty osobami uczestniczącymi w dokonywaniu tych czynności, chyba że udział tych wykonawców w postępowaniu nie utrudni uczciwej konkurencji; przepisu nie stosuje się do wykonawców, którym udziela się zamówienia na podstawie art. 62 ust. 1 pkt 2 lub art. 67 ust. 1 pkt 1 i 2;
12) Wykonawców, którzy nie wnieśli wadium do upływu terminu składania ofert, na przedłużony okres związania ofertą lub w terminie o którym mowa w art. 46 ust 3 albo nie zgodzili się na przedłużenie okresu związania ofertą;
13) Wykonawców, którzy złożyli nieprawdziwe informacje mające wpływ lub mogące mieć wpływ na wynik prowadzonego postępowania;
14) Wykonawców; którzy nie wykazali spełniania warunków udziału w postępowaniu;
15) Wykonawców, którzy należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007r.o ochronie konkurencji i konsumentów (Dz. U. Nr 50, poz. 331, z późn. zm.) złożyli odrębne oferty lub wnioski o dopuszczenie do udziału w tym samym postępowaniu, chyba że wykażą, że istniejące między nimi powiazania nie prowadza do

zachwiania uczciwej konkurencji pomiędzy Wykonawcami w postępowaniu o udzielenie zamówienia.

16) Zamawiający wyklucza z postępowania o udzielenie zamówienia wykonawcę, który w okresie 3 lat przed wszczęciem postępowania, w sposób zawiniony poważnie naruszył obowiązki zawodowe, w szczególności, gdy wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą dowolnych środków dowodowych, jeżeli zamawiający przewidział taką możliwość wykluczenia wykonawcy w ogłoszeniu o zamówieniu, w specyfikacji istotnych warunków zamówienia lub w zaproszeniu do negocjacji. Zamawiający nie wyklucza z postępowania o udzielenie zamówienia wykonawcy, który udowodni, że podjął konkretne środki techniczne, organizacyjne i kadrowe, które mają zapobiec zawinionemu i poważnemu naruszaniu obowiązków zawodowych w przyszłości oraz naprawił szkody powstałe w wyniku naruszenia obowiązków zawodowych lub zobowiązał się do ich naprawienia

B. OPIS SPOSOBU DOKONANIA OCENY SPEŁNIENIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU :

1. **Uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania.**
   Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnianie Wykonawca zobowiązany jest wykazać w sposób szczególny. Spełnienie warunku zostanie dokonane na podstawie oświadczenia o spełnianiu warunków udziału w postępowaniu.

2. **Wiedza i doświadczenie.**
   Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnianie Wykonawca zobowiązany jest wykazać w sposób szczególny. Spełnienie warunku zostanie dokonane na podstawie oświadczenia o spełnianiu warunków udziału w postępowaniu.

3. **Potencjał techniczny oraz osoby zdolne do wykonania zamówienia.**
   Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnianie Wykonawca zobowiązany jest wykazać w sposób szczególny. Spełnienie warunku zostanie dokonane na podstawie oświadczenia o spełnianiu warunków udziału w postępowaniu.

4. **Sytuacja ekonomiczna i finansowa.**
   Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnianie Wykonawca zobowiązany jest wykazać w sposób szczególny. Spełnienie warunku zostanie dokonane na podstawie oświadczenia o spełnianiu warunków udziału w postępowaniu.

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. Podmiot, który zobowiązał się do udostępnienia zasobów zgodnie z ust. 2b, odpowiada solidarnie z wykonawcą za szkodę zamawiającego powstałą wskutek nieudostępnienia tych zasobów, chyba że za nieudostępnienie zasobów nie ponosi winy.

V. WYKAZ OŚWIADCZEŃ I DOKUMENTÓW JAKIE MAJĄ DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIENIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU WYMIENIONYCH W PKT IV SPECYFIKACJI ISTOTNYCH WARUNKÓW ZAMÓWIENIA

1. W zakresie wykazania spełnienia przez Wykonawcę warunków, o których mowa w art. 22 ust.1 ustawy należy przedłożyć oświadczenie z art. 22 ust. 1 ustawy PZP – zgodnie z **załącznikiem nr 4** do SIWZ.

2. W zakresie potwierdzenia niepodlegania wykluczeniu na podstawie art. 24 ust. 1 i 2 ustawy PZP należy przedłożyć:
   1) oświadczenie o braku podstaw do wykluczenia – **Załącznik nr 5 do SIWZ**
   2) **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.**
   3) **Lista podmiotów należących do tej samej grupy kapitałowej**, o której mowa w art. 24 ust. 2 pkt 5 ustawy Pzp (załączyć tylko w przypadku przynależności do grupy kapitałowej).

3. Informacja o dokumentach potwierdzających, że oferowane usługi odpowiadają określonym wymaganiom należy przedłożyć:
   1) Formularz oferty – **Załącznik nr 3 i 3a do SIWZ.**
   2) Oświadczenie zgodnie z art. 36a ust. 1 i art. 36b ust. 1 ustawy w zakresie wskazania części zamówienia, której wykonanie zamierza powierzyć podwykonawcom – treść oświadczenia stanowi **Załącznik nr 6 do SIWZ.**
   3) Oświadczenie Wykonawcy zgodności zaoferowanego przedmiotu zamówienia z przedmiotem opisanym szczegółowo w SIWZ i jej ewentualnych zmianach - **Załącznik nr 7 do SIWZ**
   4) **Ponadto w zakresie pozycji nr 1 zamówienia wykonawca winien załączyć do oferty następujące dokumenty:**
      a) oświadczenie producenta wskazujące podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej
      b) oświadczanie Producenta lub Autoryzowanego Partnera Serwisowego o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające numer modułu internetowego i infolinii telefonicznej)
      c) certyfikat ISO 9001 podmiotu serwisującego
      d) oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późniejszymi zmianami.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

4. Dokumenty podmiotów zagranicznych

Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, przedkłada:
A. zamiast dokumentu, o którym mowa w pkt. V.2.2) SIWZ dokument wystawiony w kraju, w którym ma siedzibę lub miejsce zamieszkania potwierdzających, że:
a) nie otwarto jego likwidacji ani nie ogłoszono upadłości - wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
b) jeżeli w kraju miejsca zamieszkania osoby lub w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów o których mowa w pkt. a, zastępuje się je dokumentem 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 – wystawione z odpowiednia datą wymagana dla tych dokumentów.

5. Warunki udziału podmiotów ubiegających się wspólnie o zamówienie:

a) oferta winna być podpisana przez każdego partnera lub upoważnionego przedstawiciela / partnera wiodącego;
b) upoważnienie do pełnienia funkcji przedstawiciela / partnera wiodącego wymaga podpisu prawnie upoważnionych przedstawicieli każdego z partnerów – **należy załączyć je do oferty**;
c) Przedstawiciele / wiodący partner winien być upoważniony do zaciągania zobowiązań i płatności w imieniu każdego na rzecz każdego z partnerów oraz do wyłącznego występowania w realizacji kontraktu.
d) podmioty występujące wspólnie ponoszą solidarną odpowiedzialność za niewykonanie lub nienależyte wykonanie zobowiązań,
e) Dokumenty z pkt. **V.1 (w zakresie oświadczenia z art. 24 ust. 1 i 2) oraz z pkt. V.2.** każdy z podmiotów składa osobno, natomiast dokumenty z pkt. **V.1.** (w zakresie art. 22 ust. 1) oraz zabezpieczenie oferty wadium pkt **VI.1.,** jeżeli jest wymagane podmioty składają razem.

VI. WARUNKI WPŁATY I ZWROTU WADIUM

1. Przystępując do przetargu Wykonawca jest obowiązany wnieść wadium w wysokości **20 000,00 zł** (słownie: dwadzieścia tysięcy złotych 00/100):

2. Wadium należy wpłacić przelewem na konto Zamawiającego:
PeKaO S.A. V Oddział/Łódź 78 1240 1545 1111 0000 1166 9960

do dnia składania ofert z zaznaczeniem:
*„Wadium w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego o wartości powyżej 30 000 euro, nie przekraczającej 207 000 euro na **dostawę systemu informatycznego w oparciu o bezpieczeństwo sieciowe i usługi medyczne** dla Wojewódzkiego Szpitala Specjalistycznego im. M. Kopernika w Łodzi. Nr sprawy 155/ZP/15"*

3. Oferta zostanie uznana za zabezpieczoną, jeżeli środki z tytułu wadium faktycznie wpłyną na konto Zamawiającego do dnia składania oferty. Dowód wniesienia wadium należy dołączyć do oferty.

4. Wadium może być wniesione w pieniądzu lub innych przewidzianych w art. 45 ust. 6 ustawy Prawo Zamówień Publicznych formach. Jeżeli wadium będzie wniesione w formie gwarancji albo poręczenia to jego oryginał musi być załączony do oferty.

5. Wadium wnoszone w pieniądzu wpłaca się przelewem na rachunek bankowy wskazany przez Zamawiającego w pkt. 2.
6. Oferta nie zabezpieczona wymaganym przez ustawę wadium zostanie odrzucona.

7. Zamawiający zobowiązany jest zwrócić wadium na warunkach określonych w art. 46 ust. 1, 1a, 2, i 4 ustawy Prawo Zamówień Publicznych.

8. Wykonawca traci wadium na rzecz Zamawiającego, jeżeli zaistnieje którakolwiek z przesłanek wymienionych w art. 46 ust. 4a i ust. 5 ustawy Prawo Zamówień Publicznych.

VII. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA ZOBOWIĄZANIA

1. Zamawiający żąda od Wykonawcy, którego oferta została wybrana jako najkorzystniejsza **wniesienia zabezpieczenia należytego wykonania umowy**, zwanego dalej **"zabezpieczeniem".** Zabezpieczenie musi zostać wniesione przed podpisaniem umowy o wykonanie przedmiotu zamówienia.

2. Wykonawcy wspólnie ubiegający się o zamówienie ponoszą solidarną odpowiedzialność za wykonanie umowy i wniesienie zabezpieczenia należytego wykonania umowy.

3. Zabezpieczenie służy pokryciu roszczeń z tytułu niewykonania lub nienależytego wykonania umowy.

4. Zamawiający ustala zabezpieczenie należytego wykonania umowy na **5 % wynagrodzenia brutto złożonej oferty.**

5. Zabezpieczenie może być wnoszone według wyboru Wykonawcy w jednej lub w kilku następujących formach:
   a. pieniądzu;
   b. poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym, że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym;
   c. gwarancjach bankowych;
   d. gwarancjach ubezpieczeniowych;
   e. poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości. Zabezpieczenie wnoszone w pieniądzu wykonawca wpłaca przelewem na rachunek bankowy Zamawiającego w banku PKO SA/V oddział w Łodzi, Nr konta 78 1240 1545 1111 0000 1166 9960

6. W przypadku wniesienia wadium w pieniądzu Wykonawca może wyrazić zgodę na zaliczenie kwoty wadium na poczet zabezpieczenia.

7. Zabezpieczenie wniesione w pieniądzu, Zamawiający przechowa na oprocentowanym rachunku bankowym. Zamawiający zwróci zabezpieczenie wniesione w pieniądzu z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszt prowadzenia tego rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy Wykonawcy.

8. Zabezpieczenie należytego wykonania umowy będzie zwrócone Wykonawcy na poniższych zasadach:
   - 70 % wartości zabezpieczenia należytego wykonania umowy zostanie zwrócone w terminie 30 dni od dnia zakończenia umowy i uznania jej za wykonana należycie przez Zamawiającego,
   - 30 % wartości zabezpieczenia należytego wykonania umowy zostanie zwrócone nie później niż w 15 dniu po upływie okresu rękojmi za wady.

9. W przypadku skorzystania z prawa opcji i związanego z tym wydłużenia terminu Wykonawca zobowiązany jest wydłużyć czas trwania gwarancji z tytułu rękojmi.

VIII. OPIS KRYTERIÓW I SPOSOBU DOKONYWANIA OCENY OFERT

1. **Zamawiający będzie oceniał każdą z ofert na podstawie następujących kryteriów:**

Kryterium	Ranga
Cena	**85 %**
Czas realizacji dostawy	**10%**
Parametry techniczne	**5%**
RAZEM:	**100%**

2. **<u>Sposób obliczenia ceny oferty:</u>**

   a) Na cenę ofert składać się będą wszystkie koszty i opłaty ponoszone przez Wykonawcę do tego należy doliczyć podatek od towarów i usług konsumpcyjnych (VAT). Wykonawca kalkulując cenę zobowiązany jest uwzględnić wszelkie koszty i opłaty, w tym w szczególności koszty ubezpieczeń, kosztów transportu itp. Ceny powinny być obliczone zgodnie z podanymi wymaganiami wskazanymi w formularzu cenowym.

   b) Wykonawca, składając ofertę, jest zobowiązany poinformować zamawiającego (w Formularzu oferty), czy wybór jego oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku VAT, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku VAT.

   c) Jeżeli złożono ofertę, której wybór prowadziłby do powstania obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, do ceny najkorzystniejszej oferty lub oferty z najniższą ceną Zamawiający doliczy podatek od towarów i usług, który Zamawiający ma obowiązek rozliczyć zgodnie z obowiązującymi przepisami.

   d) Wszystkie ceny w ofercie mają być zaokrąglone <u>do dwóch miejsc</u> po przecinku, z uwzględnieniem zasad zaokrąglania liczb (tj. 5 i powyżej w górę, poniżej w dół) – dotyczy to w szczególności wartości określonych w **Załączniku nr 3 do SIWZ.**

   e) Wykonawca poda wartości netto i brutto w złotych polskich.

   f) Oferowana cena, która będzie brana pod uwagę przy ocenie ofert to cena brutto, traktowana jako ostateczna do zapłaty przez Zamawiającego, określona do dwóch miejsc po przecinku, zawierająca wszystkie koszty związane z realizacją zamówienia, wartość netto, podatek VAT.

g) Jeżeli złożono ofertę, której wybór prowadziłby do powstania obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, do ceny najkorzystniejszej oferty lub oferty z najniższą ceną Zamawiający doliczy podatek od towarów i usług, który Zamawiający ma obowiązek rozliczyć zgodnie z obowiązującymi przepisami.

3. Sposób obliczenia wartości punktowej poszczególnych kryteriów:

Sposób oceny ofert:

Przy dokonywaniu oceny ofert Zamawiający będzie stosował następujące zasady:

e) Cena – waga 85% - (C)

W kryterium **cena** zastosowany zostanie następujący wzór arytmetyczny:

$$C = N/W*85$$

Gdzie: C – liczba punktów otrzymanych w danym kryterium,
N – najniższa wartość z zaoferowanych,
W – wartość badanej oferty,

f) Czas realizacji dostawy - waga10 % (R)

Przy przyznawaniu punktów w kryterium **czas realizacji dostaw**y Zamawiający będzie posługiwała się systemem tzn.:

- czas realizacji dostawy od 0 do 21 dni – Wykonawca otrzyma 10 pkt.= 10%
- czas realizacji dostawy od 22 do 24 dni – Wykonawca otrzyma 5 pkt. = 5%
- czas realizacji dostawy 25 dni – Wykonawca otrzyma 0 pkt. = 0%

Zamawiający przyzna punkty zgodnie z oświadczeniem wykonawcy złożonym w danej ofercie. Brak możliwości przyznania punktów pośrednich.

g) Parametry techniczne – waga 5% (P)
W zakresie tego kryterium zamawiający będzie oceniał parametry techniczne systemu obsługi Zakładu Diagnostyki Obrazowej (RIS).
Oceniając to kryterium Zamawiający przyzna punkty cząstkowe, następnie zsumuje je w ramach danej oferty i otrzymane sumy punktów podstawi do podanego niżej wzoru.
Oferta może uzyskać max. 25 punktów cząstkowych.

$$P = Pmin/Pmax *5\%$$

Gdzie:
P – liczba punktów otrzymanych w danym kryterium,
Pmin – najniższa suma otrzymanych punktów cząstkowych,
Pmax – najwyższa suma otrzymanych punktów cząstkowych,

h) Ostateczną ocenę oferty będzie stanowiła suma punktów uzyskanych w poszczególnych kryteriach.

Ocena końcowa oferty:

$$O_K = C + R + P$$

Gdzie:
OK – ocena końcowa oferty,
C – ilość punktów przyznanych w kryterium cena,
R – ilość punktów przyznanych w kryterium czasu realizacji dostawy
P – ilość punktów przyznana w kryterium parametry techniczne

4. Zamawiający zawrze umowę w przedmiocie przetargu z tym Wykonawcą, którego oferta:

a) odpowiadać będzie wymaganiom określonym w ustawie prawo zamówień publicznych i specyfikacji istotnych warunków zamówienia;
b) zostanie uznana za najkorzystniejszą w oparciu o podane kryteria wyboru zdobędzie największą ilość punktów.

5. Jeżeli cena oferty wydaje się rażąco niska w stosunku do przedmiotu zamówienia i budzi wątpliwości Zamawiającego, co do możliwości wykonania przedmiotu zamówienia zgodnie z wymogami określonymi przez Zamawiającego lub wynikającymi z odrębnych przepisów, w szczególności jest niższa o 30% od wartości zamówienia lub średniej arytmetycznej cen wszystkich złożonych ofert, Zamawiający zwróci się o udzielnie wyjaśnień, w tym złożenie dowodów, dotyczących elementów oferty mających wpływ na wysokość ceny, w szczególności w zakresie:
1) oszczędności metody wykonania zamówienia, wybranych rozwiązań technicznych, wyjątkowo sprzyjających warunków wykonania zamówienia dostępnych dla wykonawcy, oryginalności projektu wykonawcy, kosztów pracy, których wartość przyjęta do ustalenia nie może być niższa od minimalnego wynagrodzenia za pracę ustalonego na podstawie art. 2 ust. 3-5 ustawy z dnia 10 października 2002r.o minimalnym wynagrodzeniu za pracę (Dz. U. NR 200,POZ. 1679, Z 2004 R. NR 240, POZ. 2407 ORAZ Z 2005 R. NR 157, POZ. 1314).
2) pomocy publicznej udzielonej na podstawie odrębnych przepisów.

OBOWIĄZEK WYKAZANIA, ŻE OFERTA NIE ZAWIERA RAŻĄCO NISKIEJ CENY, SPOCZYWA NA WYKONAWCY.

IX. MIEJSCE I TERMIN SKŁADANIA OFERT

1. Ofertę w zapieczętowanej, opatrzonej danymi Wykonawcy jak w pkt. III. 8 SIWZ i zaadresowanej na zamawiającego kopercie należy złożyć w Kancelarii Szpitala - ul. Pabianicka 62 w godz. 8.00 -15.00.

2. Ostateczny termin składania ofert upływa dnia ..14.....**08.2015 r.** do godz. **10:00**.

3. W przypadku złożenia oferty po upływie terminu określonego w pkt. 2, zamawiający niezwłocznie zwraca ofertę, która została złożona po terminie. W przypadku przesłania oferty decyduje dzień i godzina doręczenia.

4. Wykonawca może przed upływem terminu do składania ofert, zmienić lub wycofać ofertę. Wprowadzenie zmian musi być złożone według takich samych zasad, jak składana oferta, odpowiednio oznakowana dodatkowo napisem „ZMIANA". Koperty oznaczone dopiskiem „ZMIANA" zostaną otwarte przy otwieraniu oferty wykonawcy, który wprowadził zmiany i po stwierdzeniu

poprawności procedury dokonywania zmian, zostaną dołączone do oferty. Wycofanie oferty winno być poprzedzone pisemnym powiadomieniem zamawiającego o wycofaniu oferty. Oferty, które zostały wycofane nie będą otwierane i zostaną niezwłocznie odesłane do wykonawcy.

X. INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJACEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OSWIADCZEŃ I 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 istotnych warunków zamówienia wpłynął do zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert.

2. Jeżeli wniosek o wyjaśnienie treści specyfikacji istotnych warunków zamówienia wpłynął po upływie terminu składania wniosku, o którym mowa w pkt 1, lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.

3. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku, o którym mowa w pkt 1.

4. Pisemna odpowiedź na zadane zapytania zostanie przesłana jedynie tym wykonawcom, którzy pobrali pisemną wersję specyfikacji istotnych warunków zamówienia, ponadto odpowiedzi ukażą się na stronie internetowej: www.kopernik.lodz.pl.

5. Zamawiający informuje, że nie zamierza zwoływać zebrania wszystkich wykonawców w celu wyjaśnienia wątpliwości dotyczących treści specyfikacji istotnych warunków zamówienia.

6. Do kontaktów z wykonawcami w sprawach j. w. upoważnieni są:
   - w sprawach merytorycznych p. Piotr Błasiak tel. 42 689 58 90
   - w sprawach formalnych p. Małgorzata Janikowska tel. 42 689 59 11

7. Zamawiający, zgodnie z art. 27 ust. 1 ustawy dopuszcza możliwość przekazywania oświadczeń, wniosków, zawiadomień oraz informacji za pomocą:
   1. formy pisemnej (usługą pocztową),

   lub
   2. faksu: 0 42 689 54-09

   lub
   3. **poczty elektronicznej : e–mail: przetargi@kopernik.lodz.pl;**

XI. INFORMACJE DOTYCZĄCE WALUT OBCYCH

Zamawiający nie przewiduje możliwości rozliczania się z Wykonawcą w walutach obcych.

XII. TERMIN ZWIĄZANIA WARUNKAMI OFERT

Wykonawca związany jest ofertą przez okres **30 dni,** licząc od dnia upływu terminu do składania ofert.

XIII. MIEJSCE I TERMIN OTWARCIA OFERT

Komisyjne otwarcie ofert nastąpi na posiedzeniu komisji przetargowej, które odbędzie się w siedzibie Zamawiającego - Łódź, ul. Pabianicka 62, sala wykładowa **w dniu ..14.....08.2015 r. o godz. 11.00.**

XIV. ISTOTNE WARUNKI PRZYSZŁEJ UMOWY

1. Istotne warunki przyszłej umowy zostały określone w **załączniku nr 8 do SIWZ.**

2. **Przed podpisaniem umowy wykonawca zobowiązany jest dostarczyć Zamawiającemu:**
   - dokument dotyczący nadania Wykonawcy numeru NIP
   - dokument dotyczący nadania Wykonawcy numeru REGON
   - wpisu do Krajowego Rejestru Sądowego lub z centralnej ewidencji i informacji o działalności gospodarczej,
   - umowy konsorcjum, spółki cywilnej – jeżeli dotyczy.

XV. OBOWIĄZKI ZAMAWIAJĄCEGO

1. Zamawiający po otwarciu ofert, w obecności wszystkich obecnych Wykonawców, przekaże informacje, o których mowa w art. 86 ust. 4 Ustawy.
2. Niezwłocznie po wyborze oferty najkorzystniejszej oferty zamawiający zawiadomi Wykonawców, którzy złożyli oferty o:
   a) wyborze najkorzystniejszej oferty, podając nazwę (firmę), adres Wykonawcy, którego ofertę wybrano i uzasadnienie jej wyboru,
   b) adresy Wykonawców, którzy złożyli oferty wraz ze streszczeniem oceny i porównania złożonych ofert zawierających punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację.
   c) Wykonawcach, których oferty zostały odrzucone, podając uzasadnienie faktyczne i prawne,
   d) Wykonawcach którzy zostali wykluczeni z postępowania o udzielenie zamówienia, podając uzasadnienie faktyczne i prawne,
   e) terminie, określonym zgodnie z art. 94 ust. 1 lub 2, po którego upływie umowa w sprawie zamówienia publicznego może być zawarta.
3. Wszyscy Wykonawcy będą informowani o złożonych zapytaniach, zmianach terminów postępowania lub o jego unieważnieniu.
4. Umowa z Wykonawcą, którego ofertę uznano za najkorzystniejszą zostanie zawarta niezwłocznie po zakończeniu postępowania o zamówienie publiczne, zatwierdzeniu wyników przez Dyrektora WSS im. M. Kopernika i po upływie terminów, o których mowa w art. 94 ust. 1 lub 2 Ustawy.

XVI. ŚRODKI ODWOŁAWCZE PRZYSŁUGUJĄCE WYKONAWCOM W TOKU POSTĘPOWANIA

Wykonawcom przysługują środki ochrony prawnej przewidziane w Dziale VI Ustawy (art. 179 i następne).

Na Specyfikację Istotnych Warunków Zamówienia składają się następujące załączniki:

Załącznik nr 1 – szczegółowy opis przedmiotu zamówienia.
Załącznik nr 2 – strona tytułowa oferty.
Załącznik nr 3 – Formularz oferty
Załącznik nr 3a – Formularz oferty – zaoferowane parametry
Załącznik nr 4 - Oświadczenie z art. 22 ustawy pzp
Załącznik nr 5 - oświadczenie z art. 24 ustawy pzp

Załącznik nr 6 - oświadczenie w zakresie podwykonawców
Załącznik nr 7 - Oświadczenie Wykonawcy o spełnieniu warunków przedmiotowych
Załącznik nr 8 - wzór umowy

Podpisy:

.....

.....

.....

Załącznik nr 1 do SIWZ
Nr sprawy 155/ZP/15

Lp.	Przedmiot	Ilość
1.	System zabezpieczenia sieci w punkcie styku z internetem pracujący w trybie redundancji	2 systemy
2.	Przełączniki rdzeniowe	2 sztuki
3.	Rozbudowa posiadanej przez Zamawiającego obudowy HP Blade System C3000:	
3.1	Moduły LAN	4 sztuki
3.2	Karty Ethernet	6 sztuk
3.3	Moduły SAN	2 sztuki
4.	System kopii zapasowych	1 system
5.	System Obsługi Zakładu diagnostyki Obrazowej (RIS)	1 system
6.	Licencja na oprogramowanie przeglądarki medycznej obrazów DICOM	1 licencja
7.	System antywirusowy dla stacji klienckich i serwerów	1060 licencji
8.	Usługi wdrożeniowe do 31.12.2015r.	1 usługa
9.	Wsparcie utrzymaniowe	12 miesięcy – po zakończeniu usługi wdrożeniowej

Ad. 1. System zabezpieczenia sieci w punkcie styku z Internetem pracujący w trybie redundancji – 2 systemy

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
Dla elementów systemu bezpieczeństwa obsługujących WSS Kopernik w Łodzi, Wykonawca zapewni wszystkie poniższe funkcje i parametry pracy:

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive. W ramach postępowania system powinien zostać dostarczony w postaci klastra HA.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.
5. System realizujący funkcję Firewall powinien dysponować minimum 6 portami Ethernet 10/100/1000 Base-TX oraz 4 gniazdami SFP 1Gbps.
6. System powinien umożliwiać zdefiniowanie co najmniej 254 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.

7. W zakresie Firewall'a obsługa nie mniej niż 5 milionów jednoczesnych połączeń oraz 170 tys. nowych połączeń na sekundę
8. Przepustowość Firewall'a: nie mniej niż 8 Gbps dla pakietów 512 B
9. Wydajność szyfrowania VPN IPSec: nie mniej niż 7 Gbps
10. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub producenci poszczególnych elementów systemu muszą oferować systemy logowania i raportowania w postaci odpowiednio zabezpieczonych platform sprzętowych lub programowych.
11. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych:
    - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
    - Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS
    - Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN
    - Ochrona przed atakami - Intrusion Prevention System
    - Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
    - Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP
    - Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma
    - Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów)
    - Możliwość analizy ruchu szyfrowanego protokołem SSL
    - Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)
12. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 2,8 Gbps
13. Wydajność skanowania ruchu z włączoną funkcją Antywirus - minimum 1,4 Gbps
14. W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż:
    - Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
    - Praca w topologii Hub and Spoke oraz Mesh
    - Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF
    - Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
15. W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
16. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
17. Możliwość budowy minimum 8 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a., jeśli funkcja ta wymaga dodatkowej licencji należy dostarczyć ją wraz z systemem.
18. Translacja adresów NAT adresu źródłowego i docelowego.
19. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.
20. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
21. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
22. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 4500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.

23. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
24. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.
25. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
26. System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż:
    - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
    - haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
    - haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
    - Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory
27. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:
    - ICSA lub EAL4 dla funkcji Firewall
    - ICSA lub NSS Labs dla funkcji IPS
    - ICSA dla funkcji: SSL VPN, IPSec VPN
28. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
29. Serwisy i licencje
    - W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres co najmniej 24 miesięcy
30. Gwarancja oraz wsparcie

- System powinien być objęty serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, **oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej**.

- System powinien być objęty rozszerzonym serwisem gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym realizowanym przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta, w zakresie serwisu gwarancyjnego, mającego swoją siedzibę na terenie Polski.
Dla zapewnienia wysokiego poziomu usług podmiot serwisujący powinien posiadać **certyfikat ISO 9001 w zakresie świadczenia usług serwisowych**. Zgłoszenia serwisowe będą przyjmowane w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię przez minimum 8x5.
Oferent winien przedłożyć dokumenty:
- oświadczenie producenta wskazujące podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej
- oświadczanie Producenta lub Autoryzowanego Partnera Serwisowego o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające numer modułu internetowego i infolinii telefonicznej)
- certyfikat ISO 9001 podmiotu serwisującego

Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.
W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późniejszymi zmianami.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

Ad. 2 Przełączniki rdzeniowe– 2 sztuki

1.	***Obudowa***	wolnostojąca, montaż w 19-calowym stelażu telekomunikacyjnym (standard EIA) lub w specjalnej szafce na sprzęt (akcesoria montażowe w komplecie)
2.	***Ilość portów***	min. 24 RJ-45 porty automatycznego rozpoznawania 10/100/1000 (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Media Type: Auto-MDIX; Duplex: 10BASE-T/100BASE-TX: pół lub pełny; 1000BASE-T: tylko pełny; Min 4 stałe porty Gigabit Ethernet SFP Min 2 porty SFP+ 10GbE Wymagania dodatkowe: każdy z 2 portów SFP+ 10GbE musi być obsadzony modułem 10G SFP+ LC SR
3.	***Dodatkowe gniazda***	Co najmniej 2 gniazda na karty rozszerzeń dla modułów 1GbE/10GbE; Sloty SFP muszą umożliwiać instalację modułów światłowodowych zarówno 100Mb/s jak i 1000Mb/s Wymagania dodatkowe: każdy przełącznik rdzeniowy musi być wyposażony w 2 moduły 10GbE, każdy z nich wyposażony w 2 sloty SFP+ umożliwiające podłączenie kabli typu DAC 10GbE lub modułów SFP+ 10GbE.
4.	***Dodatkowe porty***	Co najmniej 1 port RJ-45 konsoli szeregowej Co najmniej 1 port RJ-45 do zarządzania poza pasmem
5.	***Zarządzanie***	Musi mieć możliwość zarządzania za pomocą: - IMC, - Web browser, - SNMP, - CLI, - Telnet - IEEE 802.3 Ethernet MIB - bezpieczny interfejs graficzny za pomocą https Musi mieć możliwość przypisywania dowolnych nazw do portów
6.	***Warstwa przełączania***	2,3
7.	***Przepustowość***	**Min.** 130Mpps
8.	***Prędkość przełączania***	**Min.** 175Gbps
9.	***Opóźnienia***	Dla 1000Mbps nie więcej niż 5 µs; Dla 10Gbps nie więcej 3 µs
10.	***Wielkość tablicy MAC***	min. 32000
11.	***Wielkość tablicy routingu***	min. 12000 wpisów (IPv4), min. 6000 wpisów (Ipv6)

12.	***Pamięć***	Co najmniej 1GB SDRAM, min. 512MB flash; packet buffor size: min. 3MB
13.	***Funkcje wysokiej dostępności***	Musi obsługiwać następujące protokoły: - Spanning Tree (802.1d), - Rapid Convergence Spanning Tree (802.1w), - Muliple Spanning Trees (802.1s) – 32 instanacje, - Per-VLAN Spanning Tree Plus (PVST+) – 128 instancji - Rapid Ring Protection Protocol (RRPP) - Device Link Detection Protocol (DLDP) - VRRP Musi mieć możliwość łączenia urządzeń stos aż do 9 urządzeń działający jako jeden wirtualny przełącznik oraz jeden wirtualny router (IRF),
14.	***Ilość obsługiwanych Vlanów***	min. 4094, wsparcie dla QinQ
15.	***Bezpieczeństwo***	W ramach bezpieczeństwa musi obsługiwać protokoły: - Radius/HWTACACS, - IEEE 802.1X - MAC-based authentication - Per-USER ACLs - Automatic VLAN assignment - SNMPv3, - SSHv2, - Guest Vlan, - STP BPDU Protection - STP Root Guard - Dynamic ARP protection - DHCP Protection, - DHCP Snooping, - DHCPv6 Snooping, - ND snooping - Endpoint Admission Defense (EAD), - Secure FTP, - Port security, - Port isolation, - IP source guard, - Ipv6 source guard, - Unicast Reverse Path Forwarding (URPF) Musi mieć możliwość tworzenia list dostępowych ACL (global ACL, VLAN ACL, port ACL, IPv6 ACL)
16.	***Auto MDIX***	Musi obsługiwać automatyczne dostosowanie prędkości na portach 10/100/1000
17.	***Agregacja portów***	zgodna z 802.3ad LACP
18.	***Monitorowanie***	Musi obsługiwać: - RMON 4 grupy statistics, history, alarm, events, - sFlow (RFC 3176),
19.	***QoS***	- Musi tworzyć klasy ruchu bazujące na listach kontroli dostępu (ACL) oraz pierwszeństwie wynikającym ze standardu IEEE 802.1p, protokołu IP, pola DSCP lub pola ToS; - musi obsługiwać funkcje filtrowania, przekierowywania, duplikowania i oznaczania; - Musi zapewniać prioryteryzację ruchu zgodną z 802.1p, ToS, TCP/UDP, możliwosc zmiany trybu obsługi kolejek w oparciu o Weigted roud robin (WRR), Weighted fair queuing (WFQ) oraz Weighted random early discard (WRED) - Storm restraint
20.	***Oprogramowanie***	Urządzenie musi mieć zapewnione bezpłatne aktualizacje przez cały okres posiadania

		sprzętu - dostępne na stronie producenta
21.	***Gwarancja***	15 lat gwarancja producenta
22.	***Serwis***	Wymiana następnego dnia roboczego na sprawne urządzenie
23.	***Redundancja zasilania***	Każdy przełącznik rdzeniowy musi być wyposażony w redundantne zasilacze o mocy min. 150W każdy.
24.	***Pozostałe funkcje***	- Routing IPv4 – statyczny i dynamiczny (min. RIP v1 i v2, OSFP, BGP) - Routing IPv6 – statyczny i dynamiczny (min. RIPng, OSFPv3, ISIS, BGP4+) - Dual flash images - Obsługa ramek Jumbo do 12288byte - tworzenie stosu do 9 urządzeń - Obsługa połączeń stack'owych za pomocą CX4, z prędkością 96Gbps - Multiple configuration files - Device Link Detection Protocol - IEEE 802.1AB Link Layer Discovery Protocol (LLDP) - LLDP-MED - LLDP-CDP compatibility - zaawansowany routing – wsparcie dla MPLS, VPLS - IEEE 802.3ah OAM - IEEE 802.3x Flow control - Voice VLAN - Multicast Source Discovery Protocol (MSDP) - Multicast Border Gateway Protocol (MBGP) - Multicast VLAN - LLDP-CDP compatibility - receives and recognizes CDP packets from Cisco's IP phones for seamless interoperation - IGMP, PIM-SM, PIM-SSM, PIM-DM, BI-PIM, MSDP - wsparcie dla OpenFlow 1.0 I 1.3 (SDN)

Ad. 3 Rozbudowa posiadanej przez Zamawiającego obudowy HP Blade System C3000

Ad. 3.1 3.1 Moduły LAN - 4 szt.

Lp.	Element konfiguracji	Wymagania minimalne
1	Typ infrastruktury	Niżej wymienione moduły muszą być kompatybilne z posiadaną przez zamawiającego Obudową HP Blade System C3000
2	Moduły LAN	Minimum 4 moduły typu 10Gb Ethernet wyprowadzające sygnały z minimum 2 portów sieciowych 10Gb na serwerach. Urządzenia te muszą umożliwiać agregację połączeń LAN w infrastrukturze blade i muszą umożliwiać wyprowadzenie sygnałów LAN z infrastruktury z zachowaniem redundancji połączeń. Każdy moduł powinien posiadać minimum 10 portów 10Gb przygotowanych do obsadzenia modułami SFP+ lub kablami połączeniowymi typu DAC 10GbE.
3	Dodatkowa funkcjonalność modułów LAN	Możliwość przydzielania adresów MAC predefiniowanych przez producenta rozwiązania blade dla poszczególnych wnęk na serwery w obudowie. Przydzielenie adresów musi powodować zastąpienie fizycznych adresów kart Ethernet na serwerze. Musi istnieć także możliwość przenoszenia przydzielonych adresów pomiędzy wnękami w obudowie. Funkcjonalność ta musi być realizowana zarówno poprzez moduły LAN w infrastrukturze lub poprzez dodatkowe oprogramowanie producenta serwerów blade. Dodatkowo

		dla sieci LAN musi istnieć możliwość stworzenia niezależnych połączeń VLAN tak aby między wydzielonymi sieciami nie było komunikacji.. Wymagane wszystkie niezbędne licencje na opisaną funkcjonalność dla całej infrastruktury blade. W przypadku sieci LAN, musi istnieć możliwość określenia pasma przepustowości pojedynczego portu LAN na serwerze od 100Mb/s do 10Gb/s.
4	Kable połączeniowe	Każdy moduł należy dostarczyć wraz z 2 szt. Kabli połączeniowych typu 10G SFP+/SFP+ o długości 3m. Kable muszą być kompatybilne zarówno z dostarczanymi modułami, jak i przełącznikami rdzeniowymi oferowanymi w ramach niniejszego postępowania.
5	Gwarancja	Zaoferowane moduły muszą być nowe, pochodzić z oficjalnego kanału sprzedaży producenta modułów oraz obudowy Blade a po zainstalowaniu w obudowie blade muszą umożliwiać objęcie gwarancją producenta na całą obudowę Blade.

Ad. 3.2 Karty Ethernet do serwerów HP BL465G7 posiadanych przez Zamawiającego– 6 szt. kart

Lp	Element konfiguracji	Wymagania minimalne
1	Interfejsy sieciowe (LAN)	Karta dwuportowa 10GbE Mezzanine z możliwością podzielenia każdego interfejsu na 4 karty sieciowe (posiadające własne adresy MAC oraz będące widoczne z poziomu systemu operacyjnego jako fizyczne karty sieciowe). Podział musi być niezależny od zainstalowanej na serwerze platformy wirtualizacyjnej. Karta musi być kompatybilna z posiadanym serwerem HP BL465G7 oraz współpracować z modułami opisanymi w powyższym punkcie - „moduły LAN – 4 szt."
2	Gwarancja	Zaoferowane interfejsy sieciowe muszą być nowe, pochodzić z oficjalnego kanału sprzedaży producenta serwerów Blade a po zainstalowaniu w serwerach muszą umożliwiać objęcie gwarancją producenta na serwery Blade.

Ad. 3.3 Moduły SAN - 2 szt.

Lp	Element konfiguracji	Wymagania minimalne
1	Moduły SAN	Switch SAN 8Gb FC w ramach obudowy umożliwiający wyprowadzenie sygnału w sposób redundantny z obydwu portów FC ze wszystkich serwerów możliwych do zainstalowania w posiadanej przez Zamawiającego obudowie Blade (po min. Jednym interfejsie na każde urządzenie SAN switch). Switche muszą być dostarczone wraz z odpowiednią ilością patchcordów LC umożliwiających połączenie ich z posiadanymi przez Zamawiającego przełącznikami SAN 8Gb/s w trybie redundancji. Moduł SAN musi być wyposażony w min. 4 wkładki FC 8Gb/s na portach zewnętrznych oraz licencję na min. 12 portów aktywnych.
2	Gwarancja	1 rok gwarancja producenta

Ad. 4 System Kopii Zapasowych.

Lp.	Rodzaj cechy	Opis cechy
1	Funkcjonalność	Oprogramowanie powinno oferować elastyczną architekturę (serwer zarządzający/ media-serwer/ klient) celem sprostania rozwojowi środowiska informatycznego Zamawiającego.
2	Funkcjonalność	Oprogramowanie musi zapisywać dane na taśmach tak zoptymalizowane, aby nie było potrzeby wykonywania żadnych dodatkowych działań (nawet automatycznych) celem ich optymalizacji.
3	Funkcjonalność	Oprogramowanie powinno umożliwiać łatwą rozbudowę w miarę rozrastania się infrastruktury informatycznej.
4	Funkcjonalność	Oprogramowanie nie może preferować dostawcy hardware dla którego dostępna jest bogatsza funkcjonalność (macierze, biblioteki taśmowe itp.). Zamawiający musi mieć możliwość zmiany producenta sprzętu bez utraty funkcjonalności backupu.
5	Funkcjonalność	Oprogramowanie powinno być łatwe w instalacji, konfigurowaniu i zarządzaniu poprzez interfejs graficzny (GUI). Oprogramowanie powinno umożliwiać pełne dostosowanie do środowiska Zamawiającego.
6	Funkcjonalność	Oprogramowanie powinno posiadać zaawansowane funkcje monitoringu oraz generator raportów.
7	Funkcjonalność	Oprogramowanie powinno umożliwiać backup po sieci LAN serwerów z Windows 2003/2008/2012 i Linux z rodziny RedHat, Suse, Ubuntu oraz Oracle Linux.
8	Funkcjonalność	Oprogramowanie powinno wykorzystywać do przechowywania danych bezobsługowe biblioteki taśmowe, dyski lokalne oraz dyski sieciowe.
9	Funkcjonalność	Oprogramowanie musi mieć możliwość stosowania go w środowisku Storage Area Network, co zapewni dużą szybkość wykonywanych backupów oraz musi posiadać funkcjonalność współdzielenia napędów taśmowych pomiędzy serwery backupowe w sieci SAN.
10	Funkcjonalność	Oprogramowanie musi posiadać możliwość równoczesnego zapisu/odczytu na wielu napędach taśmowych w tym samym czasie.
11	Funkcjonalność	Oprogramowanie musi potrafić backupować online bazy danych, np. Oracle, Exchange, Microsoft SQL.
12	Funkcjonalność	Oprogramowanie musi umożliwiać backup i odtwarzanie serwera Exchange na poziomie pojedynczej wiadomości w skrzynkach użytkowników. Opcja powinna umożliwiać odzyskiwanie z backupu bazy danych bez dodatkowego backupu skrzynek pocztowych w trybie MAPI.
13	Funkcjonalność	Oprogramowanie musi mieć wbudowany mechanizm do backupowania otwartych plików.
14	Funkcjonalność	Oprogramowanie musi potrafić wykorzystywać do backupu mechanizm kopii migawkowych systemów z rodziny Microsoft Windows (VSS).
15	Funkcjonalność	Oprogramowanie musia posiadać funkcje disaster–recovery dla systemów z rodziny Windows, umożliwiające proste i szybkie automatyczne odtworzenie serwera po awarii zapewniające integralność i spójność danych, opcja ta powinna być integralną częścią systemu backupowego.

16	Funkcjonalność	Oprogramowanie musi umożliwiać automatyczny backup bazujący na kalendarzu. Musi mieć możliwość backupu typu: full, incremental, differential.
17	Funkcjonalność	Oprogramowanie musi umożliwiać wykonywanie skryptów przed i po backupie (np. uruchamianych przed backupem bazy oraz po wykonaniu backupu off-line bazy, np.: kasowanie redo logów).
18	Funkcjonalność	Oprogramowanie musi mieć możliwość szyfrowania danych przesyłanych przez sieć LAN. Opcja powinna być ściśle zintegrowana z produktem do backupu.
19	Funkcjonalność	Oprogramowanie musi umożliwiać kompresję na kliencie backupowym przed wysłaniem danych przez sieć.
20	Funkcjonalność	Oprogramowanie musi umożliwiać pracę w klastrze serwerów z Microsoft Windows 2008 oraz 2012.
21	Funkcjonalność	Oprogramowanie musi posiadać możliwość wykonywania backupów na urządzenia dyskowe, które następnie będą automatycznie powielane na nośniki taśmowe (D2D2T). System backupowy powinien, tak długo jak dane obecne są na dyskach, wykorzystywać je w procesach restore, znacznie skracając czas odtworzenia danych.
22	Funkcjonalność	Oprogramowanie powinno oferować funkcjonalność pozwalającą zminimalizować ilość koniecznych do wykonywania powtarzalnych pełnych kopii danych systemów plików.
23	Funkcjonalność	Oprogramowanie musi umożliwiać monitowanie i alertowanie poprzez e-mail i SNMP.
24	Funkcjonalność	Oprogramowanie musi posiadać możliwość backupu online danych z systemu SharePoint Portal Server wraz z odtwarzaniem pojedynczych dokumentów z jednoprzebiegowego backupu.
25	Funkcjonalność	Oprogramowanie musi mieć możliwość zintegrowania się z technologią vStorage API celem wydajnego backupu danych z możliwością odtwarzania pojedynczych plików (zawartych w VMDK dla systemów Windows), backup musi być wykonywany jednoprzebiegowo (cały plik VMDK backupowany raz).
26	Funkcjonalność	Oprogramowanie musi wspierać najnowsze wersje środowisk VMware vSphere 4.0/5.0 lub nowsze i wspierać backup za pomocą mechanizmu vstorage API dając te same możliwości jak z wykorzystaniem mechanizmu VCB.
27	Funkcjonalność	Oprogramowanie musi posiadać wsparcie dla technologii wirtualizacyjnych firmy Microsoft (Hyper-V) z możliwością odtwarzania pojedyńczych plików z maszyn wirtualnych Windows z jednoprzebiegowego backupu. Wsparcie musi uwzględniać najnowsze wersje oprogramowania Windows 2008 R2 lub 2012 w tym R2.
28	Funkcjonalność	Oprogramowanie powinno posiadać jako opcję możliwość wykonania backupu Active Directory a następnie odzyskania pojedynczych obiektów AD bez restartu i resynchronizacji systemu. Backup ten powinien być wykonywany jednoprzebiegowo.
29	Funkcjonalność	Oprogramowanie musi mieć możliwość centralnego zarządzania serwerami (Media Serwerami) systemu backupowego z pomocą nadrzędnej konsoli.
30	Funkcjonalność	Oprogramowanie ma mieć możliwość backupu poprzez sieć SAN zasobów z serwerów Linux, tak by tylko metadane były wysyłane przez sieć LAN.
31	Funkcjonalność	Oprogramowanie musi posiadać pełne wsparcie dla backupu online MS SQL 2008/ 2010/ 2012/ 2014 także w wersjach Express.
32	Funkcjonalność	Oprogramowanie musi mieć możliwość współpracy z SCOM (Microsoft System Center Operation Manager).

33	Funkcjonalność	Oprogramowanie musi wspierać najnowsze wersje aplikacji i serwerów takich jak: Windows 2008 R2/2012 R2, Exchange 2010/2013, Domino 8.5/9, Windows 7/8/8.1.
34	Funkcjonalność	Oprogramowanie musi posiadać jako opcję (komponent, włączany działający jako integralna część aplikacji backupowej) deduplikację danych. Funkcjonalność tego modułu musi opierać się na blokowej deduplikacji danych wykonywanej online a więc w trakcie wykonywania zadania backupowego. Proces deduplikacji danych musi odbywać się na kliencie (serwerze z danymi czy aplikacją) lub na media serwerze. Konfiguracja i zarządzanie całym procesem, przełączanie miejsca deduplikacji musi odbywać się za pomocą jednej konsoli zarządzającej systemem backupowym – jedna konsola dla konfigurowania i zarządzania całością procesów backupowych i odtwarzania danych.
35	Funkcjonalność	Oprogramowanie musi umożliwiać deduplikację danych na kliencie (optymalizacja transferu danych przez siec LAN/WAN). Funkcjonalność ta musi być dostępna dla systemów Windows i Linux i nie może wymagać instalacji dodatkowych komponentów czy agentów poza oprogramowaniem klienckim systemu backupowego.
36	Funkcjonalność	Oprogramowanie musi umożliwiać opcjonalne włączenie funkcjonalności deduplikacji danych i nie może powodować konieczności doinstalowania dodatkowego oprogramowania nie tylko po stronie klienta backupu ale także media serwera (serwera systemu backupowego).
37	Funkcjonalność	Oprogramowanie musi posiadać otwarte API umożliwiające podłączanie urządzeń deduplikacyjnych innych firm.
38	Funkcjonalność	Oprogramowanie musi umożliwiać odtwarzanie pojedynczych elementów (e-maili, elementów AD, plików czy baz danych) z aplikacji Exchange, Active Directory, SharePoint i MS SQL zainstalowanych w środowiskach wirtualnych (Vmware, Hyper-V) poprzez backup całej maszyny wirtualnej – pojedynczy backup całego pliku VMDK, a odtwarzanie różnego typu (cała maszyna, plik z systemu plikowego, element aplikacji/ baza danych).
39	Funkcjonalność	Oprogramowanie musi posiadać jako opcję moduł do archiwizacji danych z Exchange i systemu plików, tak by móc przenosić część danych z tych systemów na oddzielną przestrzeń dyskową celem „odchudzenia" systemów produkcyjnych. Dane zarchiwizowane z serwerów Exchange muszą być dostępne dla poszczególnych użytkowników poprzez wtyczkę do klienta poczty - Outlook.
40	Funkcjonalność	Oprogramowanie musi wspierać najnowsze wersje produktów takich jak: Microsoft SharePoint, Microsoft Exchange, Microsoft SQL Server.
41	Funkcjonalność	Oprogramowanie musi mieć możliwość szyfrowania komunikacji pomiędzy klientem (serwerem produkcyjnym) a serwerem backupowym za pomocą SSL.
42	Funkcjonalność	Oprogramowanie musi integrować się z konsolą vCenter dając administratorowi VMware możliwość monitorowania stanu backupu maszyn wirtualnych, a także możliwość sprawdzenia poprawności kopii i jej odzyskiwalności.
43	Funkcjonalność	Oprogramowanie musi mieć wbudowaną funkcję disaster-recovery. Funkcja ta musi być dostępna dla systemów z rodziny Windows i oprócz odtwarzania systemu operacyjnego musi umożliwiać zmianę sterowników minimum do urządzeń pamięci masowych czy kart sieciowych tak by było możliwe odtworzenie systemu na innym fizycznym sprzęcie.

44	Funkcjonalność	Oprogramowanie musi mieć możliwość wykonywania konwersji P2V, B2V oraz C2V serwerów fizycznych z systemem operacyjnym z rodziny Windows na maszyny wirtualne (VMware i Hyper-V) na 3 sposoby: jeden P2V – pozwala na równoczesny backup danych i jednoczesną konwersję do pełnej maszyny wirtualnej, drugi sposób: B2V wykonuje zadanie konwersji po zakończeniu zadania backupowego oraz trzeci: C2V czyli konwersja bezpośrednia całego obrazu maszyny fizycznej w trakcie jej działania do maszyny wirtualnej bez tworzenia kopii zapasowej. Wszystkie sposoby konwersji muszą być wewnętrznymi komponentami systemu backupowego i nie mogą wymagać dodatkowych licencji czy instalacji dodatkowego oprogramowania.
45	Funkcjonalność	Oprogramowanie musi mieć możliwość zarządzania z wykorzystaniem CLI (Command Line Interface) poprzez komponent Windows PowerShell obejmująca wszystkie zadania administracyjne pokrywające się możliwościami z interfejsem graficznym w 100%.
46	Funkcjonalność	Dostarczone licencje muszą pozwalać Zamawiającemu na tworzenie granuralnych kopii zapasowych nielimitowanej ilości maszyn wirtualnych ze środowiska VMware z zainstalowanymi różnorodnymi systemami operacyjnymi w skład którego wchodzą następujące serwery fizyczne: - 3 serwery 1 procesorowe z procesorami 16 rdzeniowymi, - 1 serwer 2 procesorowy z procesorami 8 rdzeniowymi, - 2 serwery 2 procesorowe z procesorami 6 rdzeniowymi, - 1 serwer z 1 procesorem 6 rdzeniowym.
47	Funkcjonalność	Dostarczone licencje muszą pozwalać dodatkowo Zamawiającemu na tworzenie granuralnych kopii zapasowych 3 serwerów fizycznych z zainstalowanymi systemami z rodziny Windows Server oraz na tworzenie granuralnej kopii zapasowej bazy danych 1 dodatkowego serwera fizycznego z zainstalowaną bazą danych Microsoft SQL.
48	Funkcjonalność	Dostarczone licencje muszą pozwalać na tworzenie kopii zapasowych na posiadanych przez Zamawiającego 2 bibliotekach taśmowych wyposażonych w 2 napędy LTO każda.
49	Funkcjonalność	Dostarczone licencje muszą pozwalać Zamawiającemu na swobodne przenoszenie pomiędzy serwerami o takich samych konfiguracjach procesorów (np. w przypadku wymiany serwera).
50	Funkcjonalność	Licencjonowanie oprogramowania musi uwzględniać prawo (w okresie przynajmniej 3 lat) do bezpłatnej instalacji udostępnianych przez producenta nowych wersji oprogramowania, uaktualnień oraz poprawek krytycznych i opcjonalnych.

Ad.5 System Obsługi Zakładu Diagnostyki Obrazowej (RIS) – 1 system.

Minimalne wymagania funkcjonalne:

Lp.	Funkcjonalność	Rodzaj parametru (opcjonalny (O) / wymagalny (W))	Spełnia (TAK/ NIE) - wypełnić	Parametry oferowane	Punktacja	Kategoria
1.	Producent systemu RIS	W	Tak. Podać		Warunek graniczny	RIS- rdzeń
2.	Nazwa handlowa i oznaczenie wersji	W	Tak. Podać		Warunek graniczny	RIS - rdzeń
3.	Nieograniczona liczba klienckich licencji dostępowych dla użytkowników RIS	W	Tak		Warunek graniczny	RIS - rdzeń
4.	Interfejs użytkownika i pomoc kontekstowa w języku polskim	W	Tak		Warunek graniczny	RIS - rdzeń

5.	Otwarta, modularna budowa systemu. W ramach dostawy licencje wystarczające na jednoczesną pracę 30 użytkowników oraz podłączenie 30 urządzeń DICOM	W	Tak		Warunek graniczny	RIS - rdzeń
6.	Architektura typu klient-serwer oparta o asynchroniczną komunikację	W	Tak		Warunek graniczny	RIS - rdzeń
7.	Propagowanie zmian danych (min. statusów badań) w kierunku serwer -> klient	W	Tak		Warunek graniczny	RIS - rdzeń
8.	Klient webowy (typu single page application) działający na nowych przeglądarkach z HTML5/CSS3	W	Tak		Warunek graniczny	RIS - rdzeń
9.	Współpraca z systemami Windows XP/Vista/7/8, Linux, Mac OSX	W	Tak		Warunek graniczny	RIS - rdzeń
10.	Dostawca systemu RIS zapewni integrację z systemem HIS (AMMS) i PACS (INFINITT) eksploatowanymi w Szpitalu	W	Tak		Warunek graniczny	RIS - rdzeń
11.	Dostawca systemu RIS zapewni migrację niezbędnych danych z istniejących systemów PACS (INFINITT) i HIS (AMMS) do systemu RIS w celu zapewnienia spójności pracy na danych aktualnych i archiwalnych	W	Tak		Warunek graniczny	RIS - rdzeń
12.	System audytowy wersjonujący akcje w systemie pozwalający na przywrócenie poprzedniego stanu danych (np. cofnięcie usunięcia rekordu pacjenta, cofnięcie poprzedniej wersji opisu badania, możliwość przesłuchiwania poprzednich wersji opisów dźwiękowych)	W	Tak		Warunek graniczny	RIS - rdzeń
13.	Logowanie wszelkich działań w systemie	W	Tak		Warunek graniczny	RIS - rdzeń
14.	System bazuje na silniku bazodanowym ORACLE. Zamawiający posiada silnik bazodanowy.	W	Tak		Warunek graniczny	RIS - rdzeń
15.	Automatyczne wylogowanie z systemu w przypadku logowania użytkownika na innej stacji	W	Tak		Warunek graniczny	RIS - rdzeń
16.	Podział na dedykowane moduły funkcjonalne (osobne moduły dla: rejestracji, planistek, techników, radiologów, administratorów)	W	Tak		Warunek graniczny	RIS - rdzeń
17.	Historia zmian wprowadzanych przez użytkowników	W	Tak		Warunek graniczny	RIS - rdzeń
18.	Konfigurowalny system uprawnień z podziałem na dowolnie definiowane role przynajmniej na poziomie wdrożenia	W	Tak		Warunek graniczny	RIS - rdzeń
19.	Stronicowanie danych	W	Tak		Warunek graniczny	RIS - rdzeń
20.	Odwracalne łączenie rekordów pacjenta	W	Tak		Warunek graniczny	RIS - rdzeń
21.	Centralna administracja systemem, oparta o technologię Web, administracja serwerem RIS	W	Tak		Warunek graniczny	RIS-administracja systemem
22.	Automatyczny backup bazy danych	W	Tak		Warunek graniczny	RIS-administracja systemem
23.	Możliwość deaktywacji użytkownika (blokada na logowanie i pracę w systemie, przy jednoczesnym zapisaniu wszelkich działań historycznych)	W	Tak		Warunek graniczny	RIS-administracja systemem
24.	Webowy interfejs edycji szablonów wydruku opisu (.pdf)	W	Tak		Warunek graniczny	RIS-administracja systemem
25.	Moduł administracyjny brokera HL7	W	Tak		Warunek graniczny	RIS-administracja systemem

26.	Dostęp do okna administracji i konfiguracji HL7 chroniony hasłem	W	Tak		Warunek graniczny	RIS-administracja systemem
27.	Możliwość podglądu statystyk wiadomości HL7 (poprawnie obsłużonych / błędnie obsłużonych wraz z informacją o błędzie)	W	Tak		Warunek graniczny	RIS-administracja systemem
28.	Możliwość archiwizowania wiadomości HL7 w plikach logów oraz jako osobne pliki tekstowe	W	Tak		Warunek graniczny	RIS-administracja systemem
29.	Możliwość ponowienia wysyłki wybranej wiadomości HL7 oraz możliwość wymuszenia ponownego jej przetworzenia przez system RIS	W	Tak		Warunek graniczny	RIS-administracja systemem
30.	Lista pacjentów oczekujących na badanie z informacjami dotyczącymi priorytetu badania lub informacjami o przypadkach pilnych (np. pacjenci z SOR)	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
31.	Automatyczne dokumentowanie informacji o czasie rozpoczęcia/zakończenia badania i użytkowniku systemu, który badanie przeprowadzał	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
32.	Automatyczne dokumentowanie czasu trwania badania	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
33.	Możliwość ręcznego uzupełnienia danych dotyczących osób, które były obecne przy wykonaniu badania wraz z możliwością określenia funkcji osoby w badaniu bez konieczności przelogowywania się w systemie (przypadek użycia: dwóch lub więcej techników korzysta z jednego komputera)	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
34.	Możliwość uzupełnienia danych dotyczących zużytych materiałów (możliwość definiowania zestawów materiałów przypisanych do modalności)	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
35.	Możliwość uzupełniania informacji o dawkach przyjętych przez pacjenta (promieniowanie, leki)	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
36.	Możliwość dołączania dokumentów do procedury	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
37.	Możliwość zmiany nazwy procedury	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
38.	Możliwość zmiany priorytetu badania (CITO, Planowe)	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
39.	Możliwość zapisywania informacji o numerze z księgi pracowni.	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
40.	Możliwość ręcznego oznaczenia badania jako wykonane (przypadek badania USG do którego nie zostaną wysłane żadne obrazy a musi powstać opis)	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
41.	Możliwość anulowania zleconej procedury	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
42.	Możliwość drukowania opisu badania	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
43.	Możliwość zlecenia wypalenia płyty z plikami badania	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna

44.	Możliwość przypisania lekarza radiologa do wykonywanej procedury (foldery kominkowe)	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
45.	Po otwarciu edytora opisu system RIS otworzy system PACS w kontekście opisywanego badania	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
46.	Edytor opisu sprawdza pisownię (min. język polski)	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
47.	Wsparcie dla pracy w grupach – możliwość definiowania puli lekarzy opisujących np. dodanie zewnętrznej grupy „teleradiologia" z dostępem do wybranych badań	W	Tak		Warunek graniczny	RIS - Opisy badań
48.	Wyszukiwanie/sortowanie listy roboczej lekarza po minimum następujących kryteriach: PESEL, typ badania, nazwisko pacjenta, płatnik, lekarz kierujący, priorytet, czas oczekiwania	W	Tak		Warunek graniczny	RIS - Opisy badań
49.	Możliwość określenia i zapisywania rodzaju filtrów minimum po 4 parametrach dla użytkownika	W	Tak		Warunek graniczny	RIS - Opisy badań
50.	Możliwość grupowania danych po wybranym zestawie kolumn	W	Tak		Warunek graniczny	RIS - Opisy badań
51.	Możliwość śledzenia, czy badanie jest w trakcie opisywania	W	Tak		Warunek graniczny	RIS - Opisy badań
52.	Szybki filtr zawężający listę do badań przypisanych zalogowanemu użytkownikowi	W	Tak		Warunek graniczny	RIS - Opisy badań
53.	Bezpośredni dostęp do danych dotyczących pacjenta i wizyty, opisów poprzednich badań i poprzednich danych obrazowych	W	Tak		Warunek graniczny	RIS - Opisy badań
54.	Wielopoziomowe, edytowalne wzory opisów badań	W	Tak		Warunek graniczny	RIS - Opisy badań
55.	Możliwość formatowania wzorów opisów badań	W	Tak		Warunek graniczny	RIS - Opisy badań
56.	Możliwość definiowana wzorców opisowych publicznych i prywatnych (dostępnych tylko dla wybranej osoby)	W	Tak		Warunek graniczny	RIS - Opisy badań
57.	Możliwość wdrożenia praktycznie dowolnego wzoru wydruku opisu badania (dane, format, układ)	W	Tak		Warunek graniczny	RIS - Opisy badań
58.	Możliwość umieszczenia elementów graficznych na wzorze wydruku opisu badania	W	Tak		Warunek graniczny	RIS - Opisy badań
59.	Możliwość wydruku opisów badań z oznaczeniem czasu opisu i czasu wydruku	W	Tak		Warunek graniczny	RIS - Opisy badań
60.	Nagrywanie wyników badań na zewnętrznych duplikatorach (min. Rimage, Primera, Epson)	W	Tak		Warunek graniczny	RIS - Opisy badań
61.	Wersjonowanie opisu badania	W	Tak		Warunek graniczny	RIS - Opisy badań
62.	Możliwość konfiguracji dostępu do wyników badań podmiotom zewnętrznym przez dowolną przeglądarkę internetową HTML5/CSS3	O	Tak		Tak -5 pkt. Nie -0pkt.	RIS - Opisy badań
63.	Możliwość konfiguracji automatycznego wysyłania (zaszyfrowanym mailem) zaaprobowanych opisów do jednostek zlecających wykonanie badania w trybie teleradiologii	W	Tak		Warunek graniczny	RIS - Opisy badań

64.	Możliwość konfiguracji dodatkowego modułu pozwalającego na nadawanie tymczasowego dostępu do wyniku badania dla pacjenta/lekarza kierującego	W	Tak		Warunek graniczny	RIS - Opisy badań
65.	Blokada opisu badania przez wielu użytkowników z informacją przez kogo badanie jest opisywane.	W	Tak		Warunek graniczny	RIS - Opisy badań
66.	Możliwość zapisania częściowo opisanego badania jako „draft".	W	Tak		Warunek graniczny	RIS - Opisy badań
67.	Możliwość grupowania dowolnej ilości badań jednego pacjenta	W	Tak		Warunek graniczny	RIS - Opisy badań
68.	Możliwość przygotowywania jednego opisu dla wielu zgrupowanych procedur	W	Tak		Warunek graniczny	RIS - Opisy badań
69.	Kontrola jakości – możliwość oznaczenia badania jako nieczytelne wraz z możliwością określenia powodu odrzucenia	W	Tak		Warunek graniczny	RIS - Opisy badań
70.	Możliwość podglądu dokumentów dołączonych przez techników oraz rejestrację do badania	W	Tak		Warunek graniczny	RIS - Opisy badań
71.	Możliwość podglądu opisów / konsultacji do wybranego badania stworzonych w trybie teleradiologii	W	Tak		Warunek graniczny	RIS - Opisy badań
72.	Możliwość zapisania tworzonego opisu jako szablon opisowy	W	Tak		Warunek graniczny	RIS - Opisy badań
73.	Możliwość dodawania wielu opisów do jednego badania (jeden opis powinien być opisem głównym – oferowany system umożliwia ręczną zmianę wyboru opisu głównego)	W	Tak		Warunek graniczny	RIS - Opisy badań
74.	Funkcjonalność DICOM Modality Worklist	W	Tak		Warunek graniczny	RIS-interfejs DICOM
75.	Możliwość dodania/ skonfigurowania dowolnej liczby list roboczych DICOM	W	Tak		Warunek graniczny	RIS-interfejs DICOM
76.	Generowanie DICOM Modality Worklist zależnie od statusu badania	W	Tak		Warunek graniczny	RIS-interfejs DICOM
77.	Automatyczne usuwanie badania z listy DICOM z konsoli urządzenia, w momencie kiedy badanie zostanie zakończone w RIS	W	Tak		Warunek graniczny	RIS-interfejs DICOM
78.	Generowanie listy roboczej DICOM zależnie od poszczególnych typów badań	W	Tak		Warunek graniczny	RIS-interfejs DICOM
79.	Generowanie listy roboczej DICOM zależnie od poszczególnych pracowni diagnostycznych	W	Tak		Warunek graniczny	RIS-interfejs DICOM
80.	Generowanie listy roboczej DICOM zależnie od poszczególnych urządzeń diagnostycznych	W	Tak		Warunek graniczny	RIS-interfejs DICOM
81.	Dowolnie konfigurowalne mapowanie informacji z systemu RIS do tagów DICOM WORKLIST	W	Tak		Warunek graniczny	RIS-interfejs DICOM
82.	Możliwość „ręcznego" połączenia badania obrazowego DICOM z rekordem pacjenta, np. w momencie awarii listy roboczej DICOM	W	Tak		Warunek graniczny	RIS-interfejs DICOM
83.	Możliwość odbierania i komunikatów oraz ich aktualizacji zawierających informacje o zleceniu	W	Tak		Warunek graniczny	RIS-interfejs HL7
84.	Możliwość odbierania i komunikatów oraz ich aktualizacji zawierających informacje o pacjencie	W	Tak		Warunek graniczny	RIS-interfejs HL7
85.	Możliwość odbierania komunikatów ORM zawierających zlecenie wykonania kilku procedur	W	Tak		Warunek graniczny	RIS-interfejs HL7
86.	Możliwość odbierania i wysyłania komunikatów z opisem badania oraz jego aktualizacji (opis może być dodawany z poziomu dowolnego z systemów HIS / RIS / PACS)	W	Tak		Warunek graniczny	RIS-interfejs HL7

87.	Możliwość odbierania i wysyłania komunikatów potwierdzających wykonanie badania	W	Tak		Warunek graniczny	RIS-interfejs HL7
88.	Możliwość odsyłania komunikatów do systemów HIS i PACS z informacją o osobach obecnych przy wykonaniu badania (min. o lekarzu obecnym przy wykonaniu badania)	W	Tak		Warunek graniczny	RIS-interfejs HL7
89.	Możliwości wydzielenia w systemie zewnętrznych jednostek radiologicznych z osobnymi lekarzami do wsparcia teleradiologii	O	Tak		Tak - 10 pkt. Nie – 0 pkt.	RIS - Teleradiologia
90.	Oparta o reguły funkcja auto-routingu w RIS. W zależności od badań znajdujących się na liście lekarza opisującego, system może przenosić automatycznie dane obrazowe pacjenta na przypisaną do lekarza opisową stację roboczą (np. na podstawie jednostki kierującej, komórki/oddziału, rodzaju badania, kodu ICD10, lekarza kierującego itp.)	O	Tak		Tak - 10 pkt. Nie – 0 pkt.	RIS - Teleradiologia
91.	Możliwość zdefiniowania i podłączenia dowolnej liczby stacji diagnostycznych i archiwów PACS	W	Tak		Warunek graniczny	RIS - Teleradiologia

Schemat obiegu komunikacji HL7 między systemami HIS <–> RIS <–> PACS

Ad. 6. Licencja na oprogramowanie przeglądarki medycznej obrazów DICOM – 1 licecnja

Lp.	opis
1.	Viewer w wersji autorun CD/DVD • dogrywany do tworzonej na robocie płyty z obrazami DICOM, • automatycznie otwierający zawarte na płycie badania
2.	Obsługiwane różnorodne typy plików DICOM a. Radiografia cyfrowa (CR, DX) b. Mammografia (MG) c. Tomografia komputerowa (CT) d. Rezonans magnetyczny (MR) e. Pozytonowa tomografia emisyjna PET-CT (PT) - **Fuzja PET-CT** f. Ultrasonografia (US) g. Cyfrowa angiografia (XA)

	h. Gamma kamera, medycyna nuklearna (NM) i. Obrazy wtórne i zeskanowane (SC)
3.	Porównywanie różnych serii i badań
4.	Kompatybilny z systemami Windows (od Windows XP)
5.	Bez wymagań instalacji dodatkowych składników (np. .NET, Java)
6.	Bezterminowa

Ad.7. System antywirusowy dla stacji klienckich i serwerów – 1060 licencji (ochrona na minimum 36 Miesięcy).

1. Pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update.
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim.
4. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim.
5. Skuteczność programu potwierdzona nagrodami VB100 i co najmniej dwie inne niezależne organizacje takie jak ICSA labs lub Check Mark.

Ochrona antywirusowa i antyspyware

6. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
7. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
8. Wbudowana technologia do ochrony przed rootkitami.
9. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
10. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
11. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
12. 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.
13. 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).
14. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
15. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu.
16. Możliwość skanowania dysków sieciowych i dysków przenośnych.
17. Skanowanie plików spakowanych i skompresowanych.
18. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń).
19. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
20. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
21. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
22. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.

23. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
24. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
25. 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.
26. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).
27. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
28. 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).
29. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
30. Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.
31. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
32. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
33. 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.
34. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
35. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
36. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
37. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
38. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
39. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
40. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
41. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
42. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
43. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
44. 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.
45. 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.

46. 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.
47. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
48. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
49. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
50. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
51. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
52. 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.
53. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
54. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.
55. 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.
56. 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.
57. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
58. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
59. 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 , urządzeń przenośnych oraz urządzeń dowolnego typu.
60. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
61. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły.
62. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia.
63. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.

64. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
65. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika
66. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
67. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to program 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 program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach.
    - Tryb inteligentny – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.
68. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
69. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
70. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
71. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
72. 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.
73. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
74. 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.
75. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
76. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
77. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.
78. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
79. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http
80. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
81. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
82. Program ma być w pełni zgodny z technologią CISCO Network Access Control.
83. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.

84. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.
85. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.
86. 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.
87. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
88. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej.
89. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.
90. Możliwość podejrzenia licencji za pomocą, której program został aktywowany.

Ochrona serwera plików Windows

1. Wsparcie dla systemów: Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, SBS 2003, SBS 2003 R2, SBS 2008, SBS 2011, Microsoft MultiPoint Server 2010, Microsoft MultiPoint Server 2011, Windows MultiPoint Server 2012.
2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
4. Wbudowana technologia do ochrony przed rootkitami i exploitami.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
7. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu.
10. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
11. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.
12. Możliwość skanowania dysków sieciowych i dysków przenośnych.
13. Skanowanie plików spakowanych i skompresowanych.
14. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (z uwzględnieniem plików bez rozszerzeń).
15. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
16. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi.
17. Aplikacja powinna wspierać mechanizm klastrowania.
18. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
19. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.

20. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
21. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD i pamięci masowych FireWire.
22. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model i wersję modelu urządzenia.
23. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika.
24. 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.
25. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
26. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
27. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
28. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
29. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
30. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
31. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
32. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
33. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
34. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
35. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
36. 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.
37. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
38. Aktualizacje modułów analizy heurystycznej.
39. 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 będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
40. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
41. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.
42. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

43. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
44. Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej.
45. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
46. Interfejs programu ma oferować funkcję pracy w trybie bez grafiki gdzie cały interfejs wyświetlany jest w formie formatek i tekstu.
47. Interfejs programu ma mieć możliwość automatycznego aktywowania trybu bez grafiki w momencie, gdy użytkownik przełączy system Windows w tryb wysokiego kontrastu.
48. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.
49. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.
50. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo.
51. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC.
52. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
53. System antywirusowy 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. Program ma także posiadać opcję dezaktywacji tego mechanizmu.
54. Po instalacji systemu antywirusowego, 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.
55. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
56. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
57. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: stacji dyskietek, napędów CD/DVD oraz portów USB.
58. System antywirusowy 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.
59. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
60. System antywirusowy 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.
61. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
62. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
63. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
64. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).

65. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). Przykładowo, domyślny profil aktualizuje z sieci lokalnej a w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu.
66. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
67. Praca programu musi być niezauważalna dla użytkownika.
68. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.
69. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Ochrona serwera plików Linux

1. Skaner antywirusowy, antyspyware
2. Możliwość skanowania wszystkimi modułami programu (heurystyka, sygnatury, adware/spyware, aplikacje niepożądane, aplikacje niebezpieczne)
3. Skanowanie plików, plików spakowanych, archiwów samorozpakowujących, plików wiadomości e-mail
4. Konfiguracja wszystkich modułów oprogramowania ma być możliwa poprzez edycję jednego pliku konfiguracyjnego
5. Możliwość ustawień limitów dla modułu skanującego względem maksymalnego rozmiaru pliku, maksymalnej liczby warstw kompresji, maksymalnego rozmiaru archiwum, maksymalnego czasu skanowania, maksymalnego rozmiaru archiwum samorozpakowującego, rozszerzenia skanowanego pliku
6. Możliwość skanowania podkatalogów oraz podążania za łączami symbolicznymi (symlinkami) w systemie
7. Możliwość definicji maksymalnego poziomu głębokości skanowanych podkatalogów
8. Możliwość tworzenia kwarantanny dla plików zainfekowanych w dowolnej lokalizacji w systemie plików
9. Możliwość zdefiniowania częstotliwości aktualizacji programu z dokładnością do jednej minuty.
10. Brak potrzeby instalacji dodatkowych zależności do systemu oprócz biblioteki LIBC, oprogramowanie po instalacji jest od razu gotowe do pracy
11. Wbudowany bezpośrednio w program system obsługi plików spakowanych niewymagający zewnętrznych komponentów zainstalowanych w systemie
12. Brak potrzeby instalacji źródeł jądra systemu oraz kompilacji jakichkolwiek modułów jądra do skanowania plików na żądanie
13. Możliwość tworzenia przynajmniej pięciu poziomów dokładności czyszczenia zainfekowanych plików
14. Możliwość skanowania alternatywnych strumieni danych (ADS) obecnych w systemie plików NTFS
15. Wsparcie dla integracji oprogramowania z modułem Dazuko Access Controll (DAC) który odpowiada za skanowania plików w trybie on-access podczas zdarzeń typu otwarcie, zamknięcie oraz wykonanie pliku
16. Wsparcie dla skanowania za pośrednictwem biblioteki współdzielonej LIBC, która umożliwia skanowanie plików które są otwierane, zamykane lub wykonywane przez serwery plików (ftp, Samba) które wykorzystują zapytania do biblioteki LIBC
17. Możliwość zdefiniowania liczby wątków oraz liczby procesów dla każdego z modułów skanujących
18. Możliwość tworzenia różnych akcji (przynajmniej 5-ciu różnych) w zależności od typu zdarzenia (w przypadku pliku nie przeskanowanego, pliku przeskanowanego, pliku zainfekowanego).
19. Logowanie wykonanych akcji na plikach oraz zdarzeń dla poszczególnych modułów oprogramowania

20. Wsparcie dla zewnętrznego serwera logującego syslog, możliwość definiowania dowolnego pliku logu (np. daemon, mail, user itp.)
21. Możliwość zdefiniowania przynajmniej sześciu poziomów logowania programu
22. Możliwość zdefiniowania hasła zabezpieczającego służącego zabezpieczeniu podłączenia do serwera zdalnego zarządzania
23. Możliwość uruchomienia interfejsu programu dostępnego przez przeglądarkę Web
24. Interfejs ma umożliwiać modyfikację ustawień programu oraz jego aktualizację i przeskanowanie dowolnego obszaru systemu plików a także przegląd statystyk dotychczas przeskanowanych plików
25. Interfejs programu dostępny przez przeglądarkę Web wykorzystuje wbudowany w program serwer http
26. Możliwość uruchomienia interfejsu Web na dowolnym porcie TCP
27. Możliwość uruchomienia interfejsu Web na dowolnym interfejsie sieciowym
28. Możliwość zabezpieczenia dostępu do interfejsu Web poprzez zdefiniowanie nazwy użytkownika i hasła
29. Interfejs Web ma przedstawić administratorowi dokładny wynik skanowania poszczególnych plików w systemie wraz z możliwością pobrania tych wyników w postaci pliku tekstowego celem późniejszej analizy
30. Możliwość podglądu informacji o licencji bezpośrednio z poziomu interfejsu Web która zawiera przynajmniej informacje o liczbie dni do wygaśnięcia licencji, nazwę użytkownika licencji oraz pełną nazwę produktu którego dotyczy licencja
31. Program ma być wyposażony w graficzny menadżer kwarantanny dostępny z poziomu interfejsu Web. Menadżer ma oferować administratorowi możliwość przeglądu, pobrania, dodania i usunięcia plików w kwarantannie
32. Menadżer kwarantanny ma posiadać możliwość wyszukiwania plików znajdujących się w kwarantannie przynajmniej po nazwie pliku, dacie dodania pliku (możliwość definiowania przedziałów czasowych), rozmiarze (możliwość definiowania minimalnej i maksymalnej wielkości) oraz ilości plików (możliwość definiowania minimalnej i maksymalnej ilości)
33. Interfejs Web do zarządzania produktem ma opierać się o wbudowane w program biblioteki PHP w wersji nie niższej niż 5.2.8
34. Interfejs dostępny poprzez przeglądarkę Web ma umożliwiać zarządzanie programem również wtedy, gdy przeglądarka nie obsługuje kodu JavaScript
35. Możliwość stworzenia lokalnego repozytorium aktualizacji dla przynajmniej dwóch różnych produktów antywirusowych instalowanych na stacjach Windows
36. Możliwość tworzenia osobnych ustawień skanowania dla poszczególnych użytkowników w systemie
37. Możliwość definicji użytkownika systemowego z prawami którego zostanie uruchomiony demon skanujący
38. Współpraca z mechanizmem automatycznej wysyłki podejrzanych plików do laboratorium producenta
39. Wysyłka podejrzanych plików ma być możliwa bezpośrednio do producenta lub za pośrednictwem serwera zdalnego zarządzania
40. Możliwość uaktywnienia dodatkowych funkcjonalności programu (moduł skanujący pocztę e-mail oraz moduł skanujący dla bramek sieciowych) które nie wymagają od użytkownika instalacji dodatkowych zależności ani modułów a jedynie zaczytanie dodatkowych plików licencji
41. Możliwość instalacji na dowolnym systemie Linux 2.2.x, 2.4.x, 2.6.x
42. Producent ma dostarczyć pakiety instalacyjne w formacie RPM (dla dystrybucji Red Hat Mandriva, Suse oraz innych z nimi zgodnych), DEB (dla dystrybucji Debian, Ubuntu oraz innych z nimi zgodnych) oraz archiwum TGZ dla wszystkich pozostałych
43. Możliwość instalacji na systemie FreeBSD 5.x, 6.x i 7.x
44. Możliwość instalacji na systemach NetBSD oraz Solaris
45. Wsparcie dla platform 32 oraz 64 bitowych

46. Architektura programu umożliwia jego uruchomienie i optymalizację zarówno dla systemów jedno jak i wieloprocesorowych
47. System ma mieć możliwość powiadomienia administratora o wykryciu infekcji oraz powiadomienia o zbliżającym się terminie wygaśnięcia licencji za pośrednictwem poczty e-mail.
48. Możliwość szybkiej konfiguracji oprogramowania poprzez skrypt powłoki. Skrypt umożliwia prostą konfigurację oprogramowania stosownie do wykrytego systemu operacyjnego w jakim oprogramowanie zostało zainstalowane.
49. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Administracja zdalna

1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2003, 2008, 2012 oraz systemach Linux.
2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).
3. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL.
4. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika.
5. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta.
6. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.
7. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.
8. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
9. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.
10. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego.
11. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.
12. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
13. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
14. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci.
15. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny.
16. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.
17. Serwer proxy musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów na wypadek braku połączenia z serwerem centralnym.
18. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
19. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.
20. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów.
21. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.

22. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
23. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux.
24. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android.
25. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
26. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
27. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.
28. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do Serwera administracyjna zarządzającego.
29. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.
30. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
31. Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego.
32. Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny.
33. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.
34. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
35. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
36. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS.
37. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym.
38. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
39. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.
40. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
41. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.
42. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
43. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego.
44. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.
45. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera.

46. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup.
47. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
48. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
49. Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji.
50. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
51. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający.
52. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
53. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.
54. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.
55. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej.
56. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
57. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp.
58. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania.
59. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta.
60. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.
61. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś" dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku.
62. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora.
63. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta
64. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.
65. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.
66. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.
67. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp.
68. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania.
69. Serwer administracyjny musi być wyposażona w mechanizm importu oraz eksportu szablonów raportów.

70. Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostępu do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów.
71. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.
72. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.
73. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie.
74. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące.
75. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.
76. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
77. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów.
78. Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania.
79. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
80. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
81. Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
82. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.
83. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.
84. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
85. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
86. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia.
87. Serwer administracyjny musi być wyposażona w machizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana.
88. Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie).
89. Zamawiający wymaga dostarczenia serwerowego systemu operacyjnego celem zainstalowania konsoli zarządzania zdalnego.

Ad.8. Usługi wdrożeniowe

- **Zabezpieczenie punktu styku z Internetem**

Zabezpieczenie punktu styku z Internetem musi być wyposażone w zabezpieczenia typu firewall, pracujące w układzie HA i umożliwiające prace z uruchomionymi funkcjonalnościami: antywirus, antyspam, SSL VPN, IPSec ,web filtering, DLP. Powinno mieć uruchomione funkcjonalności wczesnego ostrzegania, informującego o wykryciu nieautoryzowanych obiektów, słabo zabezpieczonych punktów w sieci oraz funkcjonalności typu DLP (Data Leakage Prevention) i Anti-Malware. Klaster zapór ogniowych powinien zostać uruchomiony w trybie Active/Active jednakże zamawiający dopuści pracę w trybie Active/Pasive w wypadku gdyby konieczne było pozyskanie niezbędnych zasobów do czasu ich pozyskania przez zamawiającego. Na klastrze zapór Oferent uruchomi jedna zaporę główną (opartą o wirtualna domenę/kontekst) zabezpieczającą punkt styku z Internetem wyposażoną co najmniej w trzy strefy DMZ, Każda ze stref powinna być chroniona listami ACL wraz z odpowiednimi filtrami AV,WEB,DLP,AM,AntiSpam itd. W ramach wdrożenia należy uruchomić dodatkowo co najmniej pięć tuneli typu Client to Gateway w raz z uwierzytelnianiem w oparciu o bazę użytkowników znajdującą się na kontrolerach domeny udostępnionych do realizacji zadania przez zamawiającego (każda ingerencja w zasoby zamawiającego zostanie przed implementacją uzgodniona ze służbami IT Zamawiającego). Dodatkowo Oferent uruchomi co najmniej dwie wirtualne domeny/konteksty spełniające funkcje IPS pozwalające na wykrywanie zagrożeń i zaimplementuje je we wskazanych przez zamawiającego punktach sieci. Zapory ogniowe do sieci szkieletowej zamawiającego winny być przyłączone z wykorzystaniem zagregowanych łącz o przepływności nie mniejszej niż 4Gbit/s. Wdrożone zabezpieczenia zostaną udokumentowane przez oferenta pełna dokumentacją techniczną zawierającą opis i schematy fizycznej i logicznej topologii oraz w pełni opisaną strukturę list dostępowych wraz z ich działaniem funkcjonalnym.

- **Sieć LAN**

W ramach przebudowy środowiska sieciowego Zamawiającego z wykorzystaniem dostarczanych przełączników rdzeniowych wykonawca dokona podziału infrastruktury sieciowej na sieci logiczne oparte o VLAN'y zgodnie z podziałem ustalonym wcześniej przez Zamawiającego. Warstwa trzecia musi zostać zaterminowana na przełącznikach rdzeniowych. Od strony sieci LAN należy wygenerować odpowiednią ilość domen MSTP. Podział na klasy adresowe zostanie uzgodniony z Zamawiającym. Zamawiający nie dopuszcza aby prace związane z przebudową infrastruktury sieciowej powodowały jakąkolwiek przerwę w pracy istniejącego środowiska sieciowego oraz komunikacji zarówno pomiędzy serwerami oraz urządzeniami klienckimi. Jeżeli do wykonania zadania są niezbędne dodatkowe elementy na czas rekonfiguracji tolopogii wykonawca zobowiązany jest dostarczyć je we własnym zakresie. W całej infrastrukturze sieci LAN należy uruchomić usługi Quality of Service w oparciu o znaczniki DSCP. Wymiana ruchu w warstwie L3 i L2 pomiędzy przełącznikami rdzeniowymi musi odbywać się z wykorzystaniem łącz logicznych o przepustowości minimum 20Gbps. Wymiana tablic trasowania pomiędzy przełącznikami szkieletowymi musi następować w oparciu o dynamiczne protokoły routingu. Od strony Zasobów serwerowych Wykonawca przebuduje infrastrukturę sieciową. W ramach tej przebudowy wykorzysta zasoby sieciowe Zamawiającego. Rozbudowie podlegają tylko posiadane przez zamawiającego obudowy blade HP c3000 zgodnie ze specyfikacją sprzętową opisaną w niniejszym załączniku. Konfiguracja obudów musi być w pełni redundantna, bez tzw. Pojedynczych punktów awarii. Bazowym systemem operacyjnym znajdującym się w obudowach posiadanych przez zamawiającego jest Vmware vSphere 5.1. W ramach przebudowy wykonawca dokona upgrade'u systemów do najnowszej wersji w ramach posiadanych przez zamawiającego licencji. W ramach przebudowy i aktualizacji platformy wirtualizacyjnej Wykonawca wykona niezbędne rekonfiguracje mechanizmu VMware Site Recovery Manager uruchomionego w środowisku Zamawiającego z uwzględnieniem dostosowania planów replikacji oraz planów odzyskiwania disaster recovery do przebudowanej infrastruktury sieciowej. Przebudowa infrastruktury sieciowej od strony serwerowej musi również uwzględniać podobnie jak w przypadku sieci LAN podział na odpowiednie sieci logiczne VLAN. Ponieważ zasoby serwerowe zlokalizowane są w dwóch różnych serwerowniach należy zapewnić komunikację pomiędzy lokalizacjami zarówno na poziomi L2 jak i L3.

- **Sieć SAN**

W ramach postępowania Zamawiający wymaga przebudowy środowiska sieci SAN. Aktualnie środowisko Zamawiającego opiera się o jedną Fabrykę. Celem przebudowy i zmiany konfiguracji jest uzyskanie przez Zamawiającego pełnej redundancji środowiska SAN. W ramach przebudowy należy zainstalować i skonfigurować dodatkowe przełączniki SAN dla obudów HP c3000. Konfiguracja musi zapewniać 2 niezależne redundantne ścieżki dostępowe do zasobów storage. Zamawiający wymaga w ramach przebudowy sieci SAN rozdzielenia infrastruktury na strefy widoczności dedykowane do poszczególnych zasobów. Połączenia pomiędzy serwerowniami powinny posiadać przepustowość łączną nie mniejszą niż 32Gbps na fabrykę. Połączenia pomiędzy przełącznikami a zasobami storage powinny posiadać przepustowość łączną nie mniejszą niż 16Gbps na fabrykę.

- **Wdrożenie systemu antywirusowego**

1. Instalacja dostarczonego oprogramowania antywirusowego wraz ze wszystkimi niezbędnymi modułami na udostępnionym przez Zamawiającego serwerze
2. Konfiguracja mechanizmów zdalnego wdrażania agenta na komputerach klienckich dostosowanych do środowiska i architektury sieci Zamawiającego. Mechanizmy te muszą umożliwiać zdalne wdrożenie oprogramowania na 1060 końcówkach rozproszonych w całej sieci Zamawiającego w tym:
   a. Wymiana istniejącego oprogramowania antywirusowego na 10 serwerach należących do farmy serwerów terminalowych. Instalacja musi być przeprowadzona bez zakłócania pracy użytkowników
   b. wymiana oprogramowania antywirusowego na dwuwęzłowym klastrze serwerów plików należących do farmy serwerów terminalowych. Instalacja musi być przeprowadzona bez zakłócania pracy użytkowników.
3. Konfiguracja mechanizmów automatycznego grupowania komputerów klienckich w zależności od spełnienia przez nie określonych kryteriów. Utworzenie dynamicznych grup zgodnie z wytycznymi Zamawiającego
4. Synchronizacja listy komputerów klienckich oprogramowania antywirusowego z infrastrukturą Active Directory posiadaną przez Zamawiającego
5. Utworzenie zadań automatycznej aktualizacji bazy sygnatur wirusów
6. Konfiguracja zadań skanowania plików na serwerach plików i serwerach terminalowych.

- **Rekonfiguracja usług katalogowych Active Directory**
  a. Automatyczny mailing o zbliżającej się konieczności zmiany hasła
     i. Mailing do użytkownika o tym, że należy zmienić hasło.
     ii. Wysyłany 2 tyg. przed, tydzień przed, dzień przed wygaśnięciem hasła (daty definiuje administrator systemu)
  b. Optymalizacja obecnych polityk GPO w oparciu o filtry WMI i jednostki OU.
     i. Przegląd polityk
     ii. Eliminacja powtarzających się konfiguracji
     iii. Optymalizacja grupowania ustawień i ich podziału na polityki
     iv. Utworzenie 5 filtrów WMI
     v. Przydział polityk do filtrów
  c. Utworzenie 3 różnych polityk zarządzania hasłem (długość hasła, częstotliwość wymuszania zmiany itp.) dla jednej domeny

- **System Kopii Zapasowych**

Zamawiający wymaga instalacji oferowanego przez Wykonawcę oprogramowania do tworzenia kopii zapasowych na przygotowanym przez Zamawiającego serwerze fizycznym z systemem operacyjnym Windows Server 2008R2 i podłączonymi dwoma bibliotekami SAS z dwoma napędami LTO każda.
Zamawiający wymaga konfiguracji oferowanego przez Wykonawcę oprogramowania do tworzenia kopii zapasowych zgodnie z zaleceniami Zamawiającego, a przede wszystkim odpowiedniej konfiguracji posiadanych bibliotek taśmowych z umieszczonymi w nich taśmami oraz instalacji

odpowiednich agentów oprogramowania do tworzenia kopii zapasowych na wskazanych przez Zamawiającego serwerach fizycznych i wirtualnych.
Zamawiający wymaga utworzenia i zaimplementowania odpowiedniej polityki kopii zapasowych w oferowanym przez Wykonawcę oprogramowaniu, wykonania testów przywrócenia z utworzonej kopii zapasowej przykładowej – wskazanej przez Zamawiającego – maszyny wirtualnej, pliku z serwera z rodziny Windows Server i bazy danych Microsoft SQL.
Zamawiający wymaga od Wykonawcy przekazania wszelkich licencji do oferowanego oprogramowania w wersji elektronicznej lub papierowej potwierdzających legalność oraz spełnienie wymagań ilościowych opisanych w Specyfikacji.
Zamawiający wymaga od Wykonawcy utworzenia i przekazania pełnej dokumentacji powdrożeniowej wykonanych przy instalacji i konfiguracji prac dotyczących oferowanego oprogramowania do tworzenia kopii zapasowych.

Połączenie światłowodowe pomiędzy dwiema serwerowniami
W ramach postępowania Zamawiający wymaga wybudowania połączenia światłowodowego wielomodowego w standardzie OM4 min. 24 włókna zakończone stykiem SC w standardzie OM4. Wykonawca jest zobowiązany dostarczyć wszelkie elementy infrastruktury niezbędne do wykonania wyżej wymienionego zadania. Zamawiający przewiduje możliwość zorganizowania wizji lokalnej na życzenie Wykonawcy po uprzednim uzgodnieniu z Zamawiającym.

Ad. 9 Wsparcie utrzymaniowe.

- **Sieć LAN**
  1. Utrzymanie konfiguracji platformy sieciowej
  2. Bieżące rekonfiguracje platformy sieciowej dyktowane zmieniającym się środowiskiem Zamawiającego
  3. Nadzór aktualizacji oprogramowania urządzeń platformy Sieciowej
  4. Usuwanie i określanie problemów występujących w sieci
  5. Wsparcie dla Zamawiającego w ramach zgłoszeń uszkodzeń sprzętu u producentów
  6. Wsparcie 5x7 – czas reakcji 2 godziny
  7. Okres Wymaganego wsparcia: 12 miesięcy

- **Sieć SAN**
  1. Utrzymanie konfiguracji platformy sieci SAN
  2. Bieżące rekonfiguracje platformy sieciowej dyktowane zmieniającym się środowiskiem Zamawiającego
  3. Nadzór aktualizacji oprogramowania urządzeń platformy sieci SAN
  4. Usuwanie i określanie problemów występujących w sieci
  5. Wsparcie dla Zamawiającego w ramach zgłoszeń uszkodzeń sprzętu u producentów
  6. Wsparcie 5x7 – czas reakcji 2 godziny
  7. Okres Wymaganego wsparcia: 12 miesięcy

- **System antywirusowy**
  1. Utrzymanie platformy serwerowej i usług centralnego zarządzania systemem antywirusowym
  2. Bieżące rekonfiguracje mechanizmów wdrażania i zarządzania agentów oprogramowania antywirusowego na końcówkach dyktowane zmieniającym się środowiskiem sieci LAN Zamawiającego
  3. Nadzór procesów aktualizacji baz sygnatur oraz aktualizacji oprogramowania antywirusowego.

KOPERNIK

Załącznik nr 2 do SIWZ
Nr sprawy 155/ZP/15

STRONA TYTUŁOWA OFERTY
Nr sprawy 155/ZP/15

dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego o wartości powyżej 30 000 EURO a nie przekraczającej 207 000 euro **na dostawę systemu informatycznego w oparciu o bezpieczeństwo sieciowe i usługi medyczne** dla Wojewódzkiego Szpitala Specjalistycznego im. M. Kopernika w Łodzi.

Oznaczenie wykonawcy – nazwa	NIP
Adres (ulica, miejscowość, powiat, województwo)	Regon
Imię i nazwisko osoby prowadzącej sprawę oraz nr telefonu: Imię i nazwisko: .... nr telefonu:	Nr faksu służbowego, czynnego całą dobę, za pomocą którego zamawiający będzie przysyłał stosowne dokumenty dotyczące przedmiotowego postępowania: Nr fax: .....
Kontakt internetowy (strona www., e-mail)	Numer konta bankowego na, które należy zwrócić wadium (jeżeli było wymagane i zostało wpłacone w pieniądzu):
E-mail służbowy osoby prowadzącej sprawę:	

.....
Miejscowość / Data

.....
Podpis(y) osoby(osób) upoważnionej(ych) do podpisania niniejszej oferty w imieniu Wykonawcy(ów)

KOPERNIK

Załącznik nr 3 do SIWZ
Nr sprawy 155/ZP/15

O F E R T A

Przystępując do postepowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego o wartości powyżej 30 000 EURO a nie przekraczającej 207 000 euro **na dostawę systemu informatycznego w oparciu o bezpieczeństwo sieciowe i usługi medyczne** dla Wojewódzkiego Szpitala Specjalistycznego im. M. Kopernika w Łodzi oferujemy wykonanie zamówienia na podanych niżej warunkach:

Lp.	Przedmiot	Ilość	Jednostka miary	Cena netto jednostki miary	Wartość netto (3.x5.)	VAT (%)	Wartość brutto(6.+7.)	Nazwa oferowanego produktu/model
1.	*2.*	*3.*	*4.*	*5.*	*6.*	*7.*	*8.*	*9.*
1.	System zabezpieczenia sieci w punkcie styku z internetem pracujący w trybie redundancji	2	system					
2.	Przełączniki rdzeniowe	2	sztuka					
3.	Rozbudowa obudowy HP Blade System C3000:							
3.1	Moduły LAN	4	sztuka					
3.2	Karty Ethernet	6	sztuka					
3.3	Moduły SAN	2	sztuka					
4.	System kopii zapasowych	1	system					
5.	System Obsługi Zakładu diagnostyki Obrazowej (RIS)	1	system					
6.	Licencja na oprogramowanie przeglądarki medycznej obrazów DICOM	1	licencja					
7.	System antywirusowy dla stacji klienckich i serwerów	1060	Licencja					
8.	Usługi wdrożeniowe 31.12.2015r.	1	usługa					
9.	Wsparcie utrzymaniowe – usługa świadczona po zakończeniu usługi wdrożeniowej	12	miesiąc					
				suma				

1. **Wartość całej oferty brutto: .....PLN**

słownie: .....
PLN.

1a. Wartość oferty brutto przedmiot zamówienia od punktu (1.) do punktu (8.) tj. dostawę wraz z usługą wdrożenia:

..... zł

słownie: .....

PLN.

1b. Wartość oferty brutto za przedmiot zamówienia w zakresie punktu (9.) tj. usługi wsparcia utrzymaniowego :

..... zł

słownie: .....

PLN.

2. **Płatność realizowana będzie:**
   a) **Za przedmiot zamówienia od punktu (1.) do punktu (8.) tj. dostawę wraz z usługą wdrożenia w 12 równych miesięcznych ratach, gdzie miesięczna wysokość raty wynosi: ..... zł brutto.**

   b) **W za przedmiot zamówienia w zakresie punktu (9.) tj. usługi wsparcia utrzymaniowego w 12 równych miesięcznych ratach, gdzie miesięczna wysokość raty wynosi ..... Zł**

3. Deklarujemy **termin realizacji dostawy sprzętu, licencji i oprogramowania .....** dni od dnia zawarcia umowy. **(do 21 dni, od 22 do 24 dni, 25 dni)**

Należy uzupełnić, czas realizacji dostawy, w przypadku nie wpisania ilości dni w proponowanym czasie Zamawiający przyjmuje, że Wykonawca dopuszcza maksymalną ilość dni tj. 25.

4. Oferujemy termin płatności **(min. 60 dni)** ..... dni od dnia doręczenia faktury VAT do siedziby Zamawiającego.

5. Niniejsza oferta spełnia wymagania Specyfikacji Istotnych Warunków Zamówienia. Gwarantuję(emy) wykonanie niniejszego zamówienia zgodnie z treścią SIWZ, wyjaśnieniami do SIWZ oraz wprowadzonymi do niej zmianami.

6. Osobą upoważnioną do podpisania umowy jest: .....

7. Osobą wyznaczoną do kontaktów z Zamawiającym jest: .....

8. Adres e-mail, numer telefonu i faksu, do kontaktu Zamawiającego z Wykonawca.....

Oświadczamy, że:

1. Zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia (SIWZ) i nie wnosimy do niej zastrzeżeń, oraz oświadczamy, że uzyskaliśmy konieczne informacje do przygotowania oferty.
2. Akceptujemy w całości i bez zastrzeżeń warunki umowy zawarte we wzorze – zał. do SIWZ oraz zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia umowy w takim kształcie.
3. Uważamy się za związanych niniejszą ofertą na czas wskazany w SIWZ.

4. Pod groźbą odpowiedzialności karnej załączone do oferty dokumenty opisują stan prawny i faktyczny, aktualny na dzień otwarcia ofert (art. 233 K.K.).
5. **Nie należymy / należymy * do grupy kapitałowej** w rozumieniu ustawy z dnia 16 lutego 2007 o ochronie konkurencji i konsumentów (Dz. U. nr 50 poz. 331 z późn. zm.). W przypadku przynależności do grupy kapitałowej załączamy listę podmiotów należących do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5.
6. Oświadczamy, że wybór oferty **nie będzie/będzie** ** prowadził do powstania u Zamawiającego obowiązku podatkowego w VAT (ustawa z dnia 09.04.2015r. o zmianie ustawy o podatku od towarów i usług oraz ustawy Prawo zamówień publicznych). W przypadku powstania u Zamawiającego obowiązku podatkowego w VAT informacja winna wskazywać: nazwę, której świadczenie będzie prowadzić do powstania obowiązku podatkowego oraz wartość tej usługi bez kwoty podatku.

Lp.	Nazwa (rodzaj) towaru/usługi, których dostawa/świadczenie będzie prowadzić do powstania obowiązku podatkowego u zamawiającego	Wartość bez kwoty podatku VAT towaru/usługi
1		
2		

* niepotrzebne skreślić

** Uwaga niezaznaczenie przez wykonawcę powyższej informacji i nie wypełnienie tabeli rozumiane będzie przez zamawiającego jako informacja o tym ,że wybór oferty wykonawcy nie będzie prowadzić do powstania u zamawiającego obowiązku podatkowego.

Data .....

.....
podpis i pieczęć Wykonawcy

Nr sprawy 155/ZP/15
Załącznik nr 3a do SIWZ
Nr sprawy 155/ZP/15

Oferowane parametry w zakresie systemu obsługi Zakładu diagnostyki Obrazowej (RIS) - wypełnić

Lp.	Funkcjonalność	Rodzaj parametru (opcjonalny (O) / wymagalny (W))	Spełnia (TAK/ NIE) - wypełnić	Parametry oferowane	Punktacja	Kategoria
1.	Producent systemu RIS	W	Tak. Podać		Warunek graniczny	RIS- rdzeń
2.	Nazwa handlowa i oznaczenie wersji	W	Tak. Podać		Warunek graniczny	RIS - rdzeń
3.	Nieograniczona liczba klienckich licencji dostępowych dla użytkowników RIS	W	Tak		Warunek graniczny	RIS - rdzeń
4.	Interfejs użytkownika i pomoc kontekstowa w języku polskim	W	Tak		Warunek graniczny	RIS - rdzeń
5.	Otwarta, modularna budowa systemu. W ramach dostawy licencje wystarczające na jednoczesną pracę 30 użytkowników oraz podłączenie 30 urządzeń DICOM	W	Tak		Warunek graniczny	RIS - rdzeń
6.	Architektura typu klient-serwer oparta o asynchroniczną komunikację	W	Tak		Warunek graniczny	RIS - rdzeń
7.	Propagowanie zmian danych (min. statusów badań) w kierunku serwer -> klient	W	Tak		Warunek graniczny	RIS - rdzeń
8.	Klient webowy (typu single page application) działający na nowych przeglądarkach z HTML5/CSS3	W	Tak		Warunek graniczny	RIS - rdzeń
9.	Współpraca z systemami Windows XP/Vista/7/8, Linux, Mac OSX	W	Tak		Warunek graniczny	RIS - rdzeń
10.	Dostawca systemu RIS zapewni integrację z systemem HIS (AMMS) i PACS (INFINITT) eksploatowanymi w Szpitalu	W	Tak		Warunek graniczny	RIS - rdzeń
11.	Dostawca systemu RIS zapewni migrację niezbędnych danych z istniejących systemów PACS (INFINITT) i HIS (AMMS) do systemu RIS w celu zapewnienia spójności pracy na danych aktualnych i archiwalnych	W	Tak		Warunek graniczny	RIS - rdzeń
12.	System audytowy wersjonujący akcje w systemie pozwalający na przywrócenie poprzedniego stanu danych (np. cofnięcie usunięcia rekordu pacjenta, cofnięcie poprzedniej wersji opisu badania, możliwość przesłuchiwania poprzednich wersji opisów dźwiękowych)	W	Tak		Warunek graniczny	RIS - rdzeń
13.	Logowanie wszelkich działań w systemie	W	Tak		Warunek graniczny	RIS - rdzeń
14.	System bazuje na silniku bazodanowym ORACLE. Zamawiający posiada silnik bazodanowy.	W	Tak		Warunek graniczny	RIS - rdzeń
15.	Automatyczne wylogowanie z systemu w przypadku logowania użytkownika na innej stacji	W	Tak		Warunek graniczny	RIS - rdzeń
16.	Podział na dedykowane moduły funkcjonalne (osobne moduły dla: rejestracji, planistek, techników, radiologów, administratorów)	W	Tak		Warunek graniczny	RIS - rdzeń
17.	Historia zmian wprowadzanych przez użytkowników	W	Tak		Warunek graniczny	RIS - rdzeń

18.	Konfigurowalny system uprawnień z podziałem na dowolnie definiowane role przynajmniej na poziomie wdrożenia	W	Tak		Warunek graniczny	RIS - rdzeń
19.	Stronicowanie danych	W	Tak		Warunek graniczny	RIS - rdzeń
20.	Odwracalne łączenie rekordów pacjenta	W	Tak		Warunek graniczny	RIS - rdzeń
21.	Centralna administracja systemem, oparta o technologię Web, administracja serwerem RIS	W	Tak		Warunek graniczny	RIS-administracja systemem
22.	Automatyczny backup bazy danych	W	Tak		Warunek graniczny	RIS-administracja systemem
23.	Możliwość deaktywacji użytkownika (blokada na logowanie i pracę w systemie, przy jednoczesnym zapisaniu wszelkich działań historycznych)	W	Tak		Warunek graniczny	RIS-administracja systemem
24.	Webowy interfejs edycji szablonów wydruku opisu (.pdf)	W	Tak		Warunek graniczny	RIS-administracja systemem
25.	Moduł administracyjny brokera HL7	W	Tak		Warunek graniczny	RIS-administracja systemem
26.	Dostęp do okna administracji i konfiguracji HL7 chroniony hasłem	W	Tak		Warunek graniczny	RIS-administracja systemem
27.	Możliwość podglądu statystyk wiadomości HL7 (poprawnie obsłużonych / błędnie obsłużonych wraz z informacją o błędzie)	W	Tak		Warunek graniczny	RIS-administracja systemem
28.	Możliwość archiwizowania wiadomości HL7 w plikach logów oraz jako osobne pliki tekstowe	W	Tak		Warunek graniczny	RIS-administracja systemem
29.	Możliwość ponowienia wysyłki wybranej wiadomości HL7 oraz możliwość wymuszenia ponownego jej przetworzenia przez system RIS	W	Tak		Warunek graniczny	RIS-administracja systemem
30.	Lista pacjentów oczekujących na badanie z informacjami dotyczącymi priorytetu badania lub informacjami o przypadkach pilnych (np. pacjenci z SOR)	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
31.	Automatyczne dokumentowanie informacji o czasie rozpoczęcia/zakończenia badania i użytkowniku systemu, który badanie przeprowadzał	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
32.	Automatyczne dokumentowanie czasu trwania badania	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
33.	Możliwość ręcznego uzupełnienia danych dotyczących osób, które były obecne przy wykonaniu badania wraz z możliwością określenia funkcji osoby w badaniu bez konieczności przelogowywania się w systemie (przypadek użycia: dwóch lub więcej techników korzysta z jednego komputera)	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
34.	Możliwość uzupełnienia danych dotyczących zużytych materiałów (możliwość definiowania zestawów materiałów przypisanych do modalności)	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna

35.	Możliwość uzupełniania informacji o dawkach przyjętych przez pacjenta (promieniowanie, leki)	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
36.	Możliwość dołączania dokumentów do procedury	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
37.	Możliwość zmiany nazwy procedury	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
38.	Możliwość zmiany priorytetu badania (CITO, Planowe)	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
39.	Możliwość zapisywania informacji o numerze z księgi pracowni.	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
40.	Możliwość ręcznego oznaczenia badania jako wykonane (przypadek badania USG do którego nie zostaną wysłane żadne obrazy a musi powstać opis)	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
41.	Możliwość anulowania zleconej procedury	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
42.	Możliwość drukowania opisu badania	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
43.	Możliwość zlecenia wypalenia płyty z plikami badania	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
44.	Możliwość przypisania lekarza radiologa do wykonywanej procedury (foldery kominkowe)	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
45.	Po otwarciu edytora opisu system RIS otworzy system PACS w kontekście opisywanego badania	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
46.	Edytor opisu sprawdza pisownię (min. język polski)	W	Tak		Warunek graniczny	RIS - pracownia diagnostyczna
47.	Wsparcie dla pracy w grupach – możliwość definiowania puli lekarzy opisujących np. dodanie zewnętrznej grupy „teleradiologia" z dostępem do wybranych badań	W	Tak		Warunek graniczny	RIS - Opisy badań
48.	Wyszukiwanie/sortowanie listy roboczej lekarza po minimum następujących kryteriach: PESEL, typ badania, nazwisko pacjenta, płatnik, lekarz kierujący, priorytet, czas oczekiwania	W	Tak		Warunek graniczny	RIS - Opisy badań
49.	Możliwość określenia i zapisywania rodzaju filtrów minimum po 4 parametrach dla użytkownika	W	Tak		Warunek graniczny	RIS - Opisy badań
50.	Możliwość grupowania danych po wybranym zestawie kolumn	W	Tak		Warunek graniczny	RIS - Opisy badań
51.	Możliwość śledzenia, czy badanie jest w trakcie opisywania	W	Tak		Warunek graniczny	RIS - Opisy badań

52.	Szybki filtr zawężający listę do badań przypisanych zalogowanemu użytkownikowi	W	Tak		Warunek graniczny	RIS - Opisy badań
53.	Bezpośredni dostęp do danych dotyczących pacjenta i wizyty, opisów poprzednich badań i poprzednich danych obrazowych	W	Tak		Warunek graniczny	RIS - Opisy badań
54.	Wielopoziomowe, edytowalne wzory opisów badań	W	Tak		Warunek graniczny	RIS - Opisy badań
55.	Możliwość formatowania wzorów opisów badań	W	Tak		Warunek graniczny	RIS - Opisy badań
56.	Możliwość definiowana wzorców opisowych publicznych i prywatnych (dostępnych tylko dla wybranej osoby)	W	Tak		Warunek graniczny	RIS - Opisy badań
57.	Możliwość wdrożenia praktycznie dowolnego wzoru wydruku opisu badania (dane, format, układ)	W	Tak		Warunek graniczny	RIS - Opisy badań
58.	Możliwość umieszczenia elementów graficznych na wzorze wydruku opisu badania	W	Tak		Warunek graniczny	RIS - Opisy badań
59.	Możliwość wydruku opisów badań z oznaczeniem czasu opisu i czasu wydruku	W	Tak		Warunek graniczny	RIS - Opisy badań
60.	Nagrywanie wyników badań na zewnętrznych duplikatorach (min. Rimage, Primera, Epson)	W	Tak		Warunek graniczny	RIS - Opisy badań
61.	Wersjonowanie opisu badania	W	Tak		Warunek graniczny	RIS - Opisy badań
62.	Możliwość konfiguracji dostępu do wyników badań podmiotom zewnętrznym przez dowolną przeglądarkę internetową HTML5/CSS3	O	Tak		Tak - 5 pkt. Nie – 0 pkt.	RIS - Opisy badań
63.	Możliwość konfiguracji automatycznego wysyłania (zaszyfrowanym mailem) zaaprobowanych opisów do jednostek zlecających wykonanie badania w trybie teleradiologii	W	Tak		Warunek graniczny	RIS - Opisy badań
64.	Możliwość konfiguracji dodatkowego modułu pozwalającego na nadawanie tymczasowego dostępu do wyniku badania dla pacjenta/lekarza kierującego	W	Tak		Warunek graniczny	RIS - Opisy badań
65.	Blokada opisu badania przez wielu użytkowników z informacją przez kogo badanie jest opisywane.	W	Tak		Warunek graniczny	RIS - Opisy badań
66.	Możliwość zapisania częściowo opisanego badania jako „draft".	W	Tak		Warunek graniczny	RIS - Opisy badań
67.	Możliwość grupowania dowolnej ilości badań jednego pacjenta	W	Tak		Warunek graniczny	RIS - Opisy badań
68.	Możliwość przygotowywania jednego opisu dla wielu zgrupowanych procedur	W	Tak		Warunek graniczny	RIS - Opisy badań
69.	Kontrola jakości – możliwość oznaczenia badania jako nieczytelne wraz z możliwością określenia powodu odrzucenia	W	Tak		Warunek graniczny	RIS - Opisy badań
70.	Możliwość podglądu dokumentów dołączonych przez techników oraz rejestrację do badania	W	Tak		Warunek graniczny	RIS - Opisy badań
71.	Możliwość podglądu opisów / konsultacji do wybranego badania stworzonych w trybie teleradiologii	W	Tak		Warunek graniczny	RIS - Opisy badań
72.	Możliwość zapisania tworzonego opisu jako szablon opisowy	W	Tak		Warunek graniczny	RIS - Opisy badań
73.	Możliwość dodawania wielu opisów do jednego badania (jeden opis powinien być opisem głównym – oferowany system umożliwia ręczną zmianę wyboru opisu głównego)	W	Tak		Warunek graniczny	RIS - Opisy badań
74.	Funkcjonalność DICOM Modality Worklist	W	Tak		Warunek graniczny	RIS-interfejs DICOM

75.	Możliwość dodania/ skonfigurowania dowolnej liczby list roboczych DICOM	W	Tak		Warunek graniczny	RIS-interfejs DICOM
76.	Generowanie DICOM Modality Worklist zależnie od statusu badania	W	Tak		Warunek graniczny	RIS-interfejs DICOM
77.	Automatyczne usuwanie badania z listy DICOM z konsoli urządzenia, w momencie kiedy badanie zostanie zakończone w RIS	W	Tak		Warunek graniczny	RIS-interfejs DICOM
78.	Generowanie listy roboczej DICOM zależnie od poszczególnych typów badań	W	Tak		Warunek graniczny	RIS-interfejs DICOM
79.	Generowanie listy roboczej DICOM zależnie od poszczególnych pracowni diagnostycznych	W	Tak		Warunek graniczny	RIS-interfejs DICOM
80.	Generowanie listy roboczej DICOM zależnie od poszczególnych urządzeń diagnostycznych	W	Tak		Warunek graniczny	RIS-interfejs DICOM
81.	Dowolnie konfigurowalne mapowanie informacji z systemu RIS do tagów DICOM WORKLIST	W	Tak		Warunek graniczny	RIS-interfejs DICOM
82.	Możliwość „ręcznego" połączenia badania obrazowego DICOM z rekordem pacjenta, np. w momencie awarii listy roboczej DICOM	W	Tak		Warunek graniczny	RIS-interfejs DICOM
83.	Możliwość odbierania i komunikatów oraz ich aktualizacji zawierających informacje o zleceniu	W	Tak		Warunek graniczny	RIS-interfejs HL7
84.	Możliwość odbierania i komunikatów oraz ich aktualizacji zawierających informacje o pacjencie	W	Tak		Warunek graniczny	RIS-interfejs HL7
85.	Możliwość odbierania komunikatów ORM zawierających zlecenie wykonania kilku procedur	W	Tak		Warunek graniczny	RIS-interfejs HL7
86.	Możliwość odbierania i wysyłania komunikatów z opisem badania oraz jego aktualizacji (opis może być dodawany z poziomu dowolnego z systemów HIS / RIS / PACS)	W	Tak		Warunek graniczny	RIS-interfejs HL7
87.	Możliwość odbierania i wysyłania komunikatów potwierdzających wykonanie badania	W	Tak		Warunek graniczny	RIS-interfejs HL7
88.	Możliwość odsyłania komunikatów do systemów HIS i PACS z informacją o osobach obecnych przy wykonaniu badania (min. o lekarzu obecnym przy wykonaniu badania)	W	Tak		Warunek graniczny	RIS-interfejs HL7
89.	Możliwości wydzielenia w systemie zewnętrznych jednostek radiologicznych z osobnymi lekarzami do wsparcia teleradiologii	O	Tak		Tak - 10 pkt. Nie – 0 pkt.	RIS - Teleradiologia
90.	Oparta o reguły funkcja auto-routingu w RIS. W zależności od badań znajdujących się na liście lekarza opisującego, system może przenosić automatycznie dane obrazowe pacjenta na przypisaną do lekarza opisową stację roboczą (np. na podstawie jednostki kierującej, komórki/oddziału, rodzaju badania, kodu ICD10, lekarza kierującego itp.)	O	Tak		Tak - 10 pkt. Nie – 0 pkt.	RIS - Teleradiologia
91.	Możliwość zdefiniowania i podłączenia dowolnej liczby stacji diagnostycznych i archiwów PACS	W	Tak		Warunek graniczny	RIS - Teleradiologia

Data .....

.....
podpis i pieczęć Wykonawcy

Nr sprawy 155/ZP/15

Załącznik nr 4
Nr sprawy 155/ZP/15

(pieczęć firmowa Wykonawcy)

O Ś W I A D C Z E N I E

Zgodnie z art. 22 ust. 1 ustawy Prawo zamówień publicznych z dnia 29.01.2004 r. (tj. Dz. U. z 2013r poz. 907 z późn zm.) oświadczam, w imieniu Wykonawcy, że Wykonawca:

1. posiada uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania.

2.

posiada wiedzę i doświadczenie[1]	..... tak/nie
załącza do oferty pisemne zobowiązanie innych podmiotów do udostępnienia wiedzy i doświadczenia[2]	..... tak/nie

3.

dysponuje odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zmówienia[3]	..... tak/nie
załącza do oferty pisemne zobowiązanie innych podmiotów do udostępnienia potencjału technicznego i osób zdolnych do wykonania zamówienia[4]	..... tak/nie

4.

spełnia warunek dotyczący sytuacji ekonomicznej i finansowej[5]	..... tak/nie
załącza do oferty pisemne zobowiązanie innych podmiotów do udostępnienia sytuacji ekonomicznej i finansowej [6]	..... tak/nie

..... dn. ..... 2015r.

.....
(podpis osoby upoważnionej do
podpisania oferty)

<u>Uwaga:</u> w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia niniejsze oświadczenie winno być złożone w imieniu wszystkich Wykonawców.

[1] Należy wpisać „Tak" lub „Nie".
[2] Należy wpisać „Tak" lub „Nie" i załączyć do oferty odpowiednie zobowiązanie.
[3] Należy wpisać „Tak" lub „Nie" .
[4] Należy wpisać „Tak" lub „Nie" i załączyć do oferty odpowiednie zobowiązanie.
[5] Należy wpisać „Tak" lub „Nie".
[6] Należy wpisać „Tak" lub „Nie" i załączyć do oferty odpowiednie zobowiązanie.

Załącznik nr 5 do SIWZ
Nr sprawy 155/ZP/15

(pieczęć firmowa Wykonawcy)

O Ś W I A D C Z E N I E

Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 24 ust. 1 i 2 ustawy z dnia
29 stycznia 2004r. Prawo Zamówień Publicznych (tj. Dz. U. z 2013r. poz. 907 z późn. zm.) według którego wyklucza się:

Z postępowania o udzielenie zamówienia wyklucza się:

1) Wykonawców, w stosunku do których otwarto likwidację lub których upadłość ogłoszono, z wyjątkiem wykonawców, którzy po ogłoszeniu upadłości zawarli układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli poprzez likwidację majątku upadłego;
2) Wykonawców, którzy zalegają z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, z wyjątkiem przypadków gdy uzyskali oni przewidziane prawem zwolnienie, odroczenie, rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu;
3) osoby fizyczne, które prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przeciwko środowisku, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego;
4) spółki jawne, których wspólnika prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przeciwko środowisku, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego;
5) spółki partnerskie, których partnera lub członka zarządu prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przeciwko środowisku, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego;
6) spółki komandytowe oraz spółki komandytowo-akcyjne, których komplementariusza prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przeciwko środowisku, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego;
7) osoby prawne, których urzędującego członka organu zarządzającego prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przeciwko środowisku, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi

gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego;

8) podmioty zbiorowe, wobec których sąd orzekł zakaz ubiegania się o zamówienia, na podstawie przepisów o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary;
9) Wykonawców będących osobami fizycznymi, które prawomocnie skazano za przestępstwo, o którym mowa w art. 9 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769) – przez okres 1 roku od dnia uprawomocnienia się wyroku;
10) Wykonawców będących spółka jawna, spółka partnerska, spółka komandytowa, spółka komandytowo-akcyjna lub osoba prawna, których odpowiednio wspólnika, partnera, członka zarządu, komplementariusza lub urzędującego członka organu zarządzającego prawomocnie skazano za przestępstwo, o którym mowa w art. 9 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej – przez okres 1 roku od dnia uprawomocnienia się wyroku.
11) Wykonawców, którzy wykonywali bezpośrednio czynności związane z przygotowaniem prowadzonego postępowania, z wyłączeniem czynności wykonywanych podczas dialogu technicznego, o których mowa w art. 31a ust. 1 lub posługiwali się w celu sporządzenia oferty osobami uczestniczącymi w dokonywaniu tych czynności, chyba że udział tych wykonawców w postępowaniu nie utrudni uczciwej konkurencji; przepisu nie stosuje się do wykonawców, którym udziela się zamówienia na podstawie art. 62 ust. 1 pkt 2 lub art. 67 ust. 1 pkt 1 i 2;
12) Wykonawców, którzy nie wnieśli wadium do upływu terminu składania ofert, na przedłużony okres związania ofertą lub w terminie o którym mowa w art. 46 ust 3 albo nie zgodzili się na przedłużenie okresu związania ofertą;
13) Wykonawców, którzy złożyli nieprawdziwe informacje mające wpływ lub mogące mieć wpływ na wynik prowadzonego postępowania;
14) Wykonawców; którzy nie wykazali spełniania warunków udziału w postępowaniu;
15) Wykonawców, którzy należąc do tej samej 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.) złożyli odrębne oferty lub wnioski o dopuszczenie do udziału w tym samym postępowaniu, chyba że wykażą, że istniejące między nimi powiazania nie prowadza do zachwiania uczciwej konkurencji pomiędzy Wykonawcami w postępowaniu o udzielenie zamówienia.
16) Zamawiający wyklucza z postępowania o udzielenie zamówienia wykonawcę, który w okresie 3 lat przed wszczęciem postępowania, w sposób zawiniony poważnie naruszył obowiązki zawodowe, w szczególności, gdy wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą dowolnych środków dowodowych, jeżeli zamawiający przewidział taką możliwość wykluczenia wykonawcy w ogłoszeniu o zamówieniu, w specyfikacji istotnych warunków zamówienia lub w zaproszeniu do negocjacji. Zamawiający nie wyklucza z postępowania o udzielenie zamówienia wykonawcy, który udowodni, że podjął konkretne środki techniczne, organizacyjne i kadrowe, które mają zapobiec zawinionemu i poważnemu naruszaniu obowiązków zawodowych w przyszłości oraz naprawił szkody powstałe w wyniku naruszenia obowiązków zawodowych lub zobowiązał się do ich naprawienia.

Uwaga: Niniejsze oświadczenie składa każdy z Wykonawców wspólnie ubiegających się o udzielenie zamówienia

..... dn. ..... 2015r.

.....
(podpis osoby upoważnionej do
podpisania oferty)

KOPERNIK

WOJEWÓDZKI SZPITAL SPECJALISTYCZNY
im. M. Kopernika w Łodzi

Nr sprawy 155/ZP/15

Załącznik nr 6 do SIWZ
Nr sprawy 155/ZP/15

_____
(pieczęć firmowa Wykonawcy)

WSKAZANIE CZĘSCI ZAMÓWIENIA, KTÓREJ WYKONANIE WYKONAWCA POWIERZY PODWYKONAWCOM

Oświadczam, że **nie powierzę** podwykonawcom wykonania żadnej części zamówienia.*

Oświadczam, że **powierzę** podwykonawcom wykonanie zamówienia w następującym zakresie:*

Rodzaj części zamówienia przewidzianej do wykonania przez podwykonawcę
Nazwa podwykonawcy, o którym mowa w art. 36b Pzp 1 (jeśli dotyczy, zgodnie z rozdziałem I pkt. 9 SIWZ)

_____
*należy skreślić niewłaściwy wariant

..... dn. ..... 2015r.

.....
(podpis osoby upoważnionej do podpisania oferty)

KOPERNIK

WOJEWÓDZKI SZPITAL SPECJALISTYCZNY
im. M. Kopernika w Łodzi

Nr sprawy 155/ZP/15

Załącznik nr 7 do SIWZ
Nr sprawy 155/ZP/15

(pieczęć firmowa Wykonawcy)

O Ś W I A D C Z E N I E

Oświadczam, że **zaoferowane w przedmiotowym postepowaniu przedmiot zamówienia:**

- jest zgodny opisem przedmiotu zamówienia w specyfikacji istotnych warunków zamówienia i wprowadzonymi zmianami

- posiada wszelkie wymagane prawem dopuszczenia, zezwolenia i rejestracje wymagane na terytorium Unii Europejskiej oraz Rzeczpospolitej Polskiej.

Jednocześnie stwierdzam, iż świadom(a) jestem odpowiedzialności z art. 297 kodeksu karnego.

.....
Miejscowość / Data

.....
Podpis(y) osoby(osób) upoważnionej(ych) do podpisania niniejszej oferty w imieniu Wykonawcy(ów)

Załącznik nr 8
Nr sprawy 155/ZP/15

Wzór umowy

UMOWA NR 155/ZP/15/
z dnia _____

zawarta przez:
Wojewódzki Szpital Specjalistyczny im. M. Kopernika w Łodzi wpisany do Krajowego Rejestru Sądowego Rejestru Stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji i publicznych zakładów opieki zdrowotnej w Sądzie Rejonowym dla Łodzi – Śródmieścia w Łodzi, XX Wydział KRS pod numerem **0000004955** , REGON 000295403, NIP 729 - 23 - 45 - 599)
z siedzibą w Łodzi, ul. Pabianicka 62
reprezentowany przez .....
zwany dalej **Zamawiającym**
z
firmą .....
(REGON ..... NIP .....)
z siedzibą w ....., ulica .....,
wpisaną do ..... pod numerem .....
reprezentowaną przez.....,
zwaną dalej **Wykonawcą**
wyłonioną w wyniku postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na podstawie art. 39 w związku z art. 10 ust. Ust.1 Ustawy Prawo Zamówień Publicznych z dnia 29.01.2004 r. (Dz. U. z 2013 r. poz. 907 tekst jednolity z późn. zm.) **na dostawę systemu informatycznego w oparciu o bezpieczeństwo sieciowe i usługi medyczne** obowiązująca od dnia _____ do dnia _____o łącznej wartości ..... zł brutto (słownie: .....)

§1

1. Udzielenie zamówienia publicznego ma na celu zwiększenie bezpieczeństwa sieciowego, przepustowości sieci i poprawę jakości działania systemów informatycznych służących usługom medycznym poprzez:
   1) Dostawę systemów zabezpieczenia sieci w punkcie styku z Internetem, pracujących w trybie redundancji – 2 systemy
   2) Dostawę przełączników rdzeniowych – 2 sztuki
   3) Rozbudowę obudowy HP Blade System C3000:
      3.1) Moduły LAN- 4 sztuki
      3.2) Karty Ethernet – 6 sztuk
      3.3) Moduły SAN – 2 sztuki
   4) Dostawę systemu kopii zapasowych – 1 system
   5) Dostawę Systemu Obsługi Zakładu diagnostyki Obrazowej (RIS) – 1 system
   6) Dostawę oprogramowania przeglądarki medycznej obrazów DICOM – 1 licencja
   7) Dostawę systemów antywirusowych dla stacji klienckich i serwerów – 1060 licencji
   8) Wykonanie niezbędnych do poprawnego, niezakłóconego działania systemów i oprogramowania usług wdrożeniowych w terminie do 31.12.2015r.
   9) Świadczenie usług wsparcia utrzymaniowego przez okres 12 miesięcy - usługa świadczona po zakończeniu usługi wdrożeniowej.

   Szczegółowy opis przedmiotu zamówienia zawarty został w załączniku nr 1 do niniejszej umowy.

2. Realizacja przedmiotu zamówienia nastąpi we wskazany poniżej sposób:

a) dostawa, instalacja sprzętu, oprogramowania i licencji opisanych w § 1 pkt. 1 ppkt. od 1) do 7), zwanych w dalszej części umowy również „towarem", nastąpi w terminie ..... dni od dnia podpisania umowy;
b) usługi wdrożeniowe § 1 pkt. 1 ppkt. 8) będą wykonywane od dnia podpisania umowy do 31.12.2015r.
c) usługi wsparcia utrzymaniowego, o których mowa w § 1 pkt. 1 ppkt. 9) będą wykonywane przez okres 12 miesięcy i rozpoczną się po zakończeniu wykonywania usługi wdrożeniowej, potwierdzonego protokołem zakończenia etapu wdrożenia.

3. Zamówienia składane będą na nr faksu ..... lub e-mail: .....
4. Wykonawca dostarczy towar fabrycznie nowy, wolny od wad fizycznych i prawnych do Działu Informatyki Wojewódzkiego Szpitala Specjalistycznego im. M. Kopernika w Łodzi przy ul. Pabianickiej 62, oryginalnie zapakowany, w terminie ..... dni od dnia podpisania niniejszej umowy.
5. Wykonawca dostarczy zamówiony towar na własny koszt i ryzyko. Towar powinien być wydany w opakowaniu określonym Polskimi Normami lub normami branżowymi, a jeśli nie ma norm to w opakowaniu odpowiadającym właściwości towaru i środka transportu.
6. Wykonawca oświadcza, że dostarczany Zamawiającemu, w ramach niniejszej umowy, towar będzie przez cały okres jej obowiązywania spełniał normy jakościowe oraz parametry użytkowe zgodne z treścią złożonej przez niego oferty przetargowej oraz opisem przedmiotu zamówienia określonym w SIWZ przedmiotowego postępowania przetargowego (Znak sprawy: 155/ZP/15).
7. W przypadku stwierdzenia wad fizycznych w dostarczonym towarze, niezgodności towaru ze złożonym zamówieniem, nieprawidłowego działania towaru, Zamawiający niezwłocznie zawiadomi o tym Wykonawcę, który bezzwłocznie wymieni wadliwy towar na wolny od wad (co do jakości jak i ilości) w terminie nie dłuższym niż 5 dni roboczych od zgłoszenia danej reklamacji.

§2

1. Zamawiający zapłaci za zamówiony i dostarczony towar oraz wykonane usługi cenę brutto określoną w załączniku nr 1a do niniejszej umowy.
2. Zapłata za wykonanie umowy nastąpi w ratach we wskazany poniżej sposób:
   a) za zakres wskazany w § 1 pkt. 1 ppkt. od 1) – do 7) Zamawiający zapłaci Wykonawcy cenę .....netto..... brutto płatną w 12 równych miesięcznych ratach w wysokości po ..... **zł.** każda rata, przy czym pierwsza rata płatna będzie nie wcześniej, niż 60 dni od dnia doręczenia faktury za dostawę towaru, która zostanie wystawiona na podstawie zaakceptowanego przez Zamawiającego protokołu dostawy towaru.
   b) za zakres wskazany w § 1 pkt. 1 ppkt. 8 (usługi wdrożeniowe) zamawiający zapłaci Wykonawcy cenę ..... netto.....brutto, płatną w terminie 60 dni od dnia zakończenia usług wdrożeniowych, potwierdzonego protokołem, na podstawie prawidłowo wystawionej faktury.
   c) za zakres wskazany w § 1 pkt. 1 ppkt. 9) (usługi wsparcia) Zamawiający zapłaci Wykonawcy cenę .....netto..... brutto płatną w 12 równych miesięcznych ratach w wysokości po ..... **zł.** każda rata, przy czym pierwsza rata płatna będzie nie wcześniej, niż 01.02.2016r.
3. Zapłata nastąpi przelewem na konto bankowe Wykonawcy podane w przedłożonej przez niego Zamawiającemu, prawidłowo wystawionej fakturze VAT.
4. Za dzień zapłaty uważa się dzień obciążenia rachunku Zamawiającego.
5. Wykonawca oświadcza, że jest płatnikiem podatku od towarów i usług konsumpcyjnych VAT zobowiązanym do naliczenia i odprowadzenia podatku.
6. Zamawiający oświadcza, że oszacował ilość zamawianego towaru z należytą starannością, lecz zastrzega sobie prawo zakupu mniejszej ilości towaru od określonego w załączniku nr 1 do

niniejszej umowy z odpowiednim zmniejszeniem należności dla Wykonawcy, a Wykonawca oświadcza, że wyraża na to zgodę.

7. Termin płatności faktury dotyczącej dostawy, w której został stwierdzony wadliwy towar, rozpoczyna swój bieg od dnia wymiany wadliwego towaru na wolny od wad. Dostawa faktury korygującej nastąpi razem z dostawą towaru wolnego od wad.

§3

1. Wykonawca zobowiązuje się do zapłaty Zamawiającemu kar umownych z następujących tytułów i w wysokościach:
   a) w razie wystąpienia opóźnienia w dostawie towaru – w wysokości 0,1% wartości ceny brutto wskazanej w § 2 ust. 2 lit. a za każdy dzień opóźnienia;
   b) za dostarczenie towaru z wadami – 0,1% wartości brutto wartości ceny brutto wskazanej w § 2 ust. 2 lit. a za każdy dzień, aż do dnia wymiany wadliwego towaru na zgodny z zamówieniem co do jakości i ilości;
   c) za opóźnienie w realizacji wdrożenia powyżej 31.12.2015r. - 2 % wartości brutto wartości ceny wskazanej w § 2 ust. 2 lit. b za każdy dzień przedłużenia;
   d) opóźnienie w realizacji usługi supportu – 0,3 % wartości brutto miesięcznej raty za usługę supportu (wsparcia), za każdą rozpoczęta godzinę opóźnienia w stosunku do terminów wymaganych przez Zamawiającego;
   e) opóźnienie w zakończeniu przywrócenia pierwotnej funkcjonalności urządzeń (czas naprawy) - 2 % wartości brutto miesięcznej raty za usługę supportu (wsparcia), za każdy dzień opóźnienia.
   f) za każde stwierdzone naruszenie postanowień określonych w Załączniku nr 6 do niniejszej Umowy – 10 000zł za każde naruszenie
   g) za odstąpienie od umowy z przyczyn, za które ponosi odpowiedzialność Wykonawca 10% wartości brutto całego przedmiotu zamówienia;

2. Jeżeli szkoda Zamawiającego przekracza wysokość naliczonych kar, Zamawiający może dochodzić odszkodowania uzupełniającego na zasadach ogólnych.
3. Zamawiający ma prawo potrącenia wymagalnych należności z tytułu kar umownych z wzajemnych wierzytelności Wykonawcy wynikających z wystawionych przez niego faktur lub z wymagalnych rat.

§ 4

Zamawiający na podstawie art. 144 ust. 1 ustawy z dnia 29 stycznia 2004. prawo zamówień publicznych przewiduje możliwość dokonania zmiany w zawartej umowie w następujących sytuacjach:

1) wprowadzenia towaru zmodyfikowanego lub udoskonalonego spełniającego parametry wymagane w SIWZ, pod warunkiem zachowania ceny jednostkowej netto na poziomie nie wyższym, niż towar objęty zamówieniem początkowym (wycena poszczególnych programów, licencji, sprzętu etc. objętych zamówieniem początkowym znajduje się w załączniku nr 2). Ewentualna zmiana produktu może być dokonana poprzez zawarcie aneksu w formie pisemnej pod rygorem nieważności.
2) wycofania towaru z produkcji. Wykonawca ma obowiązek zapewnić dostarczenie towaru zamiennego o parametrach nie gorszych od towaru objętego umową pod warunkiem zachowania ceny jednostkowej netto na poziomie nie wyższym, niż produkt objęty zamówieniem początkowym. Ewentualna zmiana produktu może być dokonana poprzez zawarcie aneksu w formie pisemnej pod rygorem nieważności.
3) zmianie stawki podatku VAT w dniu wystawienia faktury za dany zakres przedmiotu zamówienia, przy czym zmianie ulega jedynie cena brutto danego zakresu, cena netto pozostaje bez zmian. Nowe stawki będą obowiązywać strony wraz z wejściem w życie przepisów je regulujących. Każdorazowa zmiana nie wymaga sporządzenia aneksu w formie pisemnej, ewentualnie strony mogą zawrzeć aneks porządkujący na wniosek Zamawiającego,
4) w przypadku zmiany wysokości minimalnego wynagrodzenia za pracę ustalonego na podstawie art. 2 ust. 3-5 ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę, bądź zmiany zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne,

Zamawiający dopuszcza podwyżkę ceny usług wsparcia, pod warunkiem, że Wykonawca w sposób nie budzący wątpliwości wykaże, że zmiany powyższe mają wpływ na koszty wykonania usług wsparcia przez wykonawcę, wraz z dokładnym wyliczeniem wskazującym na uzasadniony zakres podwyżki. Zmiana nastąpi w drodze aneksu w formie pisemnej pod rygorem nieważności.

5) zmiany polegającej na zamianie części towaru objętego zamówieniem (np. zamówienie większej ilości jednego rodzaju licencji przy rezygnacji z innych towarów) z zastrzeżeniem, iż całkowita wartość brutto umowy nie może ulec zmianie, zmiana nastąpi w formie aneksu do umowy w formie pisemnej, pod rygorem nieważności.
6) zmiana cen na korzyść Zamawiającego – jest dopuszczalna w każdym przypadku, zmiana nastąpi w formie aneksu do umowy w formie pisemnej pod rygorem nieważności,
7) zmiana terminu dostawy towaru z przyczyn niezawinionych przez Wykonawcę, po uzyskaniu zgody Zamawiającego, zmiana nastąpi w formie aneksu do umowy w formie pisemnej pod rygorem nieważności.

§5

1. Zamawiający nie ponosi odpowiedzialności za zobowiązania wynikające z umów zawartych przez Wykonawcę z osobami trzecimi (podwykonawcami).
2. Wykonawca oświadcza, że nie będzie zlecał innym podmiotom bez zgody Zamawiającego jakichkolwiek prac wynikających z postanowień niniejszej Umowy w trakcie których zaistnieje możliwość dostępu do danych osobowych przetwarzanych w serwisowanym urządzeniu, z zastrzeżeniem, że nie jest wymagana odrębna zgoda na podwykonawców ujawnionych w ofercie. Zlecenie prac, o których mowa w zdaniu poprzednim będzie możliwe po spełnieniu wymagań niniejszego paragrafu.
3. Przed rozpoczęciem usług, o których mowa w ust. 2, Zamawiający zobowiązuje Wykonawcę do spełnienia jednego z poniższych warunków:
   a) podpisania trójstronnej (Zamawiający, Wykonawca, Podwykonawca) umowy powierzenia przetwarzania danych osobowych gwarantującej bezpieczeństwo informacji w tym danych osobowych na odpowiednim poziomie nie niższym niż określono w niniejszej umowie w zakresie wskazanym w ofercie przez Wykonawcę. Zamawiającemu przysługuje prawo odmowy podpisania takiej umowy w przypadku nie spełnienia tego warunku. Zamawiający zastrzega sobie prawo wypowiedzenia umowy trójstronnej w przypadku naruszenia zasad ochrony powierzonych do przetwarzania danych osobowych przez Podwykonawcę. W takim wypadku Wykonawca zobowiązany jest do zaprzestania podpowierzania przetwarzanych danych osobowych.

   lub

   b) w przypadku powierzenia przetwarzania danych podwykonawcy, Zamawiający wyraża zgodę aby dane osobowe przetwarzane były przy udziale podwykonawcy, jednocześnie Wykonawca zobowiązuje się, że podpowierzenie danych osobowych będzie dokonane zgodnie z obowiązującymi przepisami prawa regulującymi zasady przetwarzania danych osobowych, w szczególności do zawarcia umowy podpowierzenia przetwarzania danych osobowych z podwykonawcą z zachowaniem zasad i warunków przetwarzania danych osobowych określonych w niniejszej umowie oraz gwarantującą poziom ochrony danych osobowych nie niższy niż określony w niniejszej umowie. Wykonawca ponosi wobec Zamawiającego odpowiedzialność za podwykonawcę z tytułu nieprzestrzegania przez podwykonawcę obowiązków w zakresie ochrony danych osobowych i zobowiązuje się do zapłaty kary umownej zgodnie z zapisem §3 ust. 1 lit. f umowy.

Strony ustalają, że wszelkie prace prowadzone z wykorzystaniem zdalnego dostępu, będą wykonywali uprawnieni inżynierowie Zamawiającego lub jego podwykonawcy spełniający kryteria określone przez Zamawiającego.
Zamawiający zastrzega sobie prawo cofnięcia zgody na przetwarzanie danych osobowych przez podwykonawcę w przypadku naruszenia zasad ochrony powierzonych do przetwarzania danych

osobowych przez Podwykonawcę. W takim wypadku Wykonawca zobowiązany jest do niezwłocznego zaprzestania podpowierzania przetwarzanych danych osobowych.

4. O wszelkich zmianach w zakresie podwykonawstwa w szczególności w zakresie podpowierzenia przetwarzania danych osobowych Wykonawca jest zobowiązany do niezwłocznego informowania Zamawiającego.

§6

1. Każda ze stron zobowiązana jest :
   a) powiadomić niezwłocznie drugą stronę o zmianach organizacyjno – prawnych, które miały miejsce w okresie związania umową, jeśli mają wpływ na realizację umowy lub sposób wystawiania dokumentów rozliczeniowych,
   b) złożyć komplet dokumentów wskazujących następcę prawnego.

   Niepowiadomienie przez Wykonawcę o wskazanych zmianach nie będzie powodować negatywnych skutków po stronie Zamawiającego.
2. Wykonawca nie może w jakikolwiek sposób, pod rygorem nieważności takiej czynności, przenieść wierzytelności wynikającej z niniejszej umowy, w szczególności w drodze cesji, poręczenia lub factoringu, na osobę trzecią bez uprzedniej pisemnej zgody Zamawiającego oraz bez spełnienia warunków wynikających z przepisów powszechnie obowiązującego prawa. Każda czynność mająca na celu lub skutkująca zmianą wierzyciela Zamawiającego może nastąpić dopiero po uprzednim wyrażeniu zgody przez podmiot tworzący, zgodnie z art. 54 ust. 5 ustawyo działalności leczniczej z dnia 15 kwietnia 2011 r.
3. Osobą odpowiedzialną za realizację umowy ze strony Zamawiającego jest Kierownik Działu Informatyki ..... lub osoba przez niego upoważniona. Tel. 42 689-....., fax 42 689-....., e-mail. informatyka@kopernik.lodz.pl
4. Osobą odpowiedzialną merytorycznie za realizację umowy ze strony Wykonawcy jest .....

§7

1.Zamawiającemu przysługuje prawo do:
a) odstąpienia od umowy w zakresie, dotyczącym dostawy towaru – w przypadkach powtarzających się opóźnień w dostawie towaru (co najmniej 4) lub powtarzających się dostaw towaru wadliwego (co najmniej 4). Prawo odstąpienia przysługuje Zamawiającemu w terminie 30 dni od dnia zaistnienia przyczyny. Odstąpienia dokonuje się na piśmie. Odstąpienie ma skutek na przyszłość (nie niweczy dotychczasowych dostaw). Zamawiający ma prawo wskazać zakres odstąpienia.
b) odstąpienia od umowy w zakresie, dotyczącym usługi wdrożenia – w przypadku, gdy Wykonawca nie podejmuje działań wdrożeniowych, lub podejmuje je w czasie wskazującym na to, że nie zostaną one zakończone w terminie, lub podejmuje je nienależycie. Prawo odstąpienia przysługuje Zamawiającemu w terminie 30 dni od dnia zaistnienia przyczyny. Odstąpienia dokonuje się na piśmie.
C) Wypowiedzenia umowy w zakresie, dotyczącym usług wsparcia, z zachowaniem 7-dniowego terminu wypowiedzenia - w razie co najmniej 3- krotnego niewykonywania lub nienależytego wykonywania usługi supportu

2.Zamawiający zastrzega sobie prawo do odstąpienia od umowy w terminie 30 dni od powzięcia wiadomości o istotnej zmianie okoliczności powodującej, iż wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zwarcia umowy.
3.Zamawiający ma prawo rozwiązać umowę w całości lub w części w razie pogorszenia sytuacji finansowej Zamawiającego w trakcie trwania umowy – za zapłatą ceny należnej za dostawy lub usługi wykonane do dnia rozwiązania.

§ 8

1. Zabezpieczenie należytego wykonania umowy stanowi kwota w wysokości 5 % wynagrodzenia brutto, o którym mowa w preambule Umowy, tj. kwota ..... **PLN** (słownie: ..... zł).

2. Wykonawca wniósł w dniu ..... r., ustaloną w ust. 1 kwotę zabezpieczenia, w formie .....
3. Zabezpieczenie należytego wykonania umowy będzie zwrócone Wykonawcy na poniższych zasadach:
    a. 70 % wartości zabezpieczenia należytego wykonania umowy zostanie zwrócone w terminie 30 dni od dnia zakończenia umowy i uznania jej za wykonana należycie przez Zamawiającego,
    b. 30 % wartości zabezpieczenia należytego wykonania umowy zostanie zwrócone nie później niż w 15 dniu po upływie okresu rękojmi za wady towaru będącego przedmiotem dostawy, przy czym strony wydłużają okres rękojmi za wady do lat 3 od dnia dostawy.
4. Zmiana formy zabezpieczenia dokonana może być w formie aneksu do niniejszej umowy.

§9

1. Wszelkie informacje, uzyskane przez Wykonawcę w związku z realizacją niniejszej umowy, Wykonawca powinien traktować jako poufne. Wykonawca zobowiązany jest do zachowania poufności informacji w trakcie obowiązywania umowy oraz po jej zakończeniu.
2. Wykonawca zobowiązuje się do przestrzegania, w zakresie adekwatnym do przedmiotu niniejszej Umowy, Polityki Bezpieczeństwa Informacji obowiązującej u Zamawiającego.
3. W sytuacji, w której naruszenie poufności informacji lub Polityki Bezpieczeństwa Informacji spowoduje szkodę po stronie Zamawiającego, Wykonawca zobowiązany jest do jej naprawienia na zasadach ogólnych.
4. Zamawiający zastrzega sobie prawo do dokonania auditu u Wykonawcy zgodnie normy EN:ISO 9001:2008 oraz normą ISO 27001:2007.
5. Zamawiający powierza Wykonawcy przetwarzanie danych osobowych na zasadach określonych w Załączniku nr 6 do niniejszej umowy.

§10

1. W kwestiach spornych wynikłych w związku z treścią lub realizacją niniejszej umowy strony będą dążyły do polubownego załatwienia sprawy, a gdy okaże się to niemożliwe, właściwym miejscowo będzie sąd powszechny ze względu na siedzibę Zamawiającego.
2. W sprawach nieuregulowanych niniejszą umową, zastosowanie mają przepisy Kodeksu Cywilnego i Ustawy Prawo Zamówień Publicznych. Strony wyłączają jednak między sobą zastosowanie art. 552 KC.
3. Wykonawca oświadcza, że przyjmuje do wiadomości informację o złym stanie majątkowym Zamawiającego w rozumieniu dyspozycji z art. 490 § 2 ustawy k.c.
4. Umowę sporządzono w trzech jednobrzmiących egzemplarzach dwa egzemplarze dla Szpitala i jeden dla Wykonawcy.

Załączniki:
Załącznik nr 1 – szczegółowy opis przedmiotu zamówienia;
Załącznik nr 2 – formularz ofertowy asortymentowo - cenowy
Załącznik nr 3 – wpis do Krajowego Rejestru Sądowego lub innego rejestru;
Załącznik nr 4 – dokument dotyczący nadanie Wykonawcy numeru NIP;
Załącznik nr 5 – dokument dotyczący nadanie Wykonawcy numeru REGON.
Załącznik nr 6 – Powierzenie przetwarzania danych osobowych,
Załącznik nr 7 – Oświadczenie o zachowaniu poufności

Wykonawca **Zamawiający**

Zasady powierzenia przetwarzania danych osobowych

Zważywszy, że na nośnikach informacji stanowiących części składowe lub przynależności urządzeń objętych Umową mogą znajdować się dane osobowe pacjentów oraz personelu,

Zważywszy, że niektóre z wykonywanych w ramach Umowy czynności uwarunkowane są koniecznością zapewnienia dostępu do przedmiotowych nośników i znajdujących się na nich informacji, w tym danych osobowych,

Strony widząc konieczność zawarcia umowy o powierzaniu przetwarzania danych osobowych, zgodnie z przepisem art. 31 ust. 1 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (zwaną dalej UODO) postanawiają, co następuje:

§ 1

1. Zamawiający jako Administrator Danych Osobowych gromadzonych w urządzeniach medycznych wskazanych w §1 Umowy przetwarza:
   - dane osobowe pacjentów:
   a) dane zwykłe: imiona i nazwisko, nr PESEL, data urodzenia, nr historii choroby
   b) dane wrażliwe: jednostkowe dane medyczne,
   - dane osobowe zwykłe personelu Zamawiającego: imię i nazwisko
   zwane łącznie „Danymi"
2. Zamawiający powierza Wykonawcy przetwarzanie Danych określonych w ust.1 niniejszego paragrafu tylko i wyłącznie w celu realizacji Umowy.
3. Wykonawca oświadcza, że powierzone Dane nie będą poddawane dalszemu przetwarzaniu w sposób niezgodny z celem określonym w ust. 2powyżej. Wykonawca oświadcza jednocześnie, że nie będzie przetwarzał powierzonych Danych w celach własnych.

4. **Zabrania się Wykonawcy wykonywania kopii, gromadzenia, lub przechowywania jakichkolwiek danych, których administratorem jest Szpital, z wyłączeniem gdy:**
   - będzie to niezbędne w celu realizacji umowy na zlecenie Zamawiającego

   - będą tworzone kopie bezpieczeństwa zgodnie.
5. Strony wyłączają możliwość udostępnienia przez Wykonawcę powierzonych do przetwarzania Danych osobom nieupoważnionym, innym podmiotom w tym również podmiotom powiązanym (spółki macierzyste, kapitałowe, etc.)bez zgody Zamawiającego.
6. Za udostępnienie, o którym mowa w ust. 5 należy rozumieć:

   a) przekazanie informacji lub nośnika z Danymi,
   b) weryfikację Danych,
   c) wyzbycie się Danych,
   d) powierzenie Danych,
   e) umożliwienie wglądu do Danych,
   f) upublicznienie Danych.

Zasady powierzenia przetwarzania danych osobowych

7. Wykonawca zobowiązuje się, że powierzone do przetwarzania dane osobowe nie zostaną przekazane do państwa trzeciego w rozumieniu przepisu art. 47 ustawy o ochronie danych osobowych.
8. W przypadku konieczności korzystania przez Wykonawcę z podwykonawców Zamawiający wyraża zgodę na udział podwykonawców z zastrzeżeniem, że przed rozpoczęciem usług, w których podwykonawca będzie miał dostęp do powierzonych do przetwarzania danych osobowych, Wykonawcaz obowiązuje do zawarcia umowy podpowierzenia przetwarzania danych osobowych zaakceptowany przez Zamawiającego. Podpowierzenie danych osobowych będzie dokonane zgodnie z obowiązującymi przepisami prawa regulującymi zasady przetwarzania danych osobowych, a umowa podpowierzenia będzie gwarantowała poziom ochrony danych osobowych nie niższy niż określony w niniejszej umowie. Wykonawca ponosi wobec Zamawiającego odpowiedzialność za Podwykonawcę z tytułu nieprzestrzegania przez Podwykonawcę obowiązków w zakresie ochrony danych osobowych i zobowiązuje się do zapłaty kary umownej zgodnie z postanowieniami niniejszej Umowy.

§ 2

1. Wykonawca oświadcza, że:
   a) dysponuje środkami umożliwiającymi prawidłowe przetwarzanie i zabezpieczenie danych osobowych, o których mowa w art. 36 - 39 ustawy z dnia 29.08.1997 o ochronie danych osobowych (Dz.U. z 2014 poz. 1182z późn.zm.) i są one wdrożone,
   b) spełnia wymagania określone w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczny służące do przetwarzania Danych (Dz.U.2004. Nr 100 poz.1024 z późn.zm.).

   W zakresie przestrzegania tych przepisów Wykonawca ponosi odpowiedzialność jak administrator danych.
2. Wykonawca zobowiązuje się do stosowania określonych w ust. 1 środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych będących przedmiotem przetwarzania w tym w szczególności do:
   - przygotowania i wdrożenia dokumentacji ochrony danych osobowych,
   - wyznaczenia administratora bezpieczeństwa informacji (ABI) nadzorującego przestrzeganie zasad ochrony danych osobowych, chyba że administrator danych sam wykonuje te czynności.
3. W przypadku uchylenia lub zmian przepisów, o których mowa w ust. 1, Wykonawca zobowiązuje się do respektowania i przestrzegania norm prawnych zastępujących dotychczasowe przepisy.

§ 3

1. Wykonawca zobowiązuje się do zachowania w tajemnicy wszelkich informacji, które uzyska w trakcie realizacji niniejszej umowy, chyba że obowiązek taki będzie wynikać z przepisów prawa, z zastrzeżeniem, że w zakresie, w jakim to będzie możliwe, zawiadomi o tym Zamawiającego, co najmniej dwa dni robocze przed takim ujawnieniem.
2. Wykonawca zobowiązuje się do zachowania poufności informacji, o których jest mowa w ust.1 w czasie trwania umowy i 5 lat po jej zakończeniu, zaś w przypadku Danych zachowaniu ich w poufności bezterminowo.
3. Wykonawca ponosi pełną odpowiedzialność za zachowanie poufnego charakteru wszelkich

informacji, do których uzyskał dostęp w trakcie świadczenia usług gwarancyjnych i wykonywania czynności serwisowych przez osoby świadczące pracę na jego rzecz, w jakiejkolwiek formie. Wykonawca podejmie również odpowiednie kroki dla zapewnienia zachowania poufności ww. informacji przez osoby wykonujące w jego imieniu obowiązki w ramach niniejszej umowy.

4. W przypadku naruszenia zasad poufności danych osobowych Wykonawca niezwłocznie powiadomi Administratora Bezpieczeństwa Informacji Zamawiającego lub inną osobę wskazaną przez Zamawiającego.
5. Zamawiający zastrzega sobie prawo przeprowadzenia u Wykonawcy i Podwykonawcy kontroli w zakresie ochrony przetwarzanych danych osobowych po uprzednim pisemnym powiadomieniu Wykonawcy, podczas zwykłych godzin pracy, zgodnie ze stosownym prawem w zakresie ochrony danych.
6. Wykonawca zobowiązuje się do umożliwienia Zamawiającemu przeprowadzenia kontroli w zakresie ochrony powierzonych do przetwarzania Danych. Kontrola nie może ani w sposób nieuzasadniony zakłócać działalności Wykonawcy ani naruszać żadnej z umów dotyczących poufności zawartych przez Wykonawcę ze stronami trzecimi.

§ 4

1. Osobami uprawnionym do wykonywania prac serwisowych są upoważnieni pracownicy Wykonawcy zwani dalej serwisantami.
2. Wykonawca przekaże Zamawiającemu listę osób upoważnionych przez Wykonawcę do wykonywania prac serwisowych (serwisanci) oraz zobowiązuje się do informowania o wszelkich zmianach w tym zakresie z zachowaniem formy pisemnej. Wykonawca ponosi odpowiedzialność za wszelkie wyrządzone szkody przez nieuprawnione działanie osób, którym wycofał uprawnienia a nie poinformował o tym Zamawiającego.

3. Wykonawca oświadcza, że serwisanci, o których mowa w ust. 1 są przeszkoleni z zakresu ochrony danych osobowych i posiadają upoważnienie do przetwarzania danych osobowych zgodnie z obowiązującymi aktami prawnymi związanych z ochroną danych osobowych. Upoważnieni inżynierowie przed przystąpieniem do prac serwisowych/napraw złożą stosowne Oświadczenia o zachowaniu poufności informacji uzyskanych w trakcie wykonywania czynności związanych z realizacją Umowy stanowiące Załącznik nr 7 do Umowy.

4. Zamawiający zastrzega sobie prawo do niedopuszczenia do prac na terenie Zamawiającego (przegląd serwisowy, naprawa itp.) osób nie figurujących na liście określonej w ust. 1.
5. Wykonawca oświadcza, że podczas prac serwisowych wymagających dostępu do aplikacji lub serwerów każdy z serwisantów będzie korzystał z indywidualnego konta zgodnie z obowiązującymi przepisami prawa.

6. Wykonawca zobowiązuje się do przedstawienia Zamawiającemu raportu po każdej czynności serwisowej/naprawie jeżeli w ramach wykonywanych były wykonywane operacje na zbiorach danych osobowych. Raport będzie zawierał informacje o błędach w przetwarzaniu danych jeśli takowe wystąpiły.
7. W przypadku konieczności wymiany (lub zabrania do serwisu w celu naprawy) serwisowanego urządzenia lub nośników informacji zamontowanych w tym urządzeniu (dyski, pamięci masowe itp.), na których mogły być gromadzone dane osobowe Wykonawca zobowiązuje się w chwili wymiany lub zabrania urządzenia do naprawy, do demontażu i przekazania nośników Zamawiającemu nieodpłatnie.
8. **Zaleca się by Wykonawca każdorazowo przed przystąpieniem Wykonawcy do wykonywania jakiejkolwiek usługi serwisowej objętej którąkolwiek z Umów, wykonał**

Zasady powierzenia przetwarzania danych osobowych

kopię bezpieczeństwa danych. Wykonawca odpowiada za utratę ww. danych podczas wykonywania usług serwisowych,w tym za koszty odtworzenia utraconych danych.

§ 5

1. Zamawiający wyraża zgodę na zestawienie połączenia zdalnego dostępu jeżeli będzie to niezbędne do realizacji Umowy. W celu zapewnienia poufności, integralności danych podczas połączenia przy użyciu systemu zdalnego dostępu Wykonawca zapewnia, że będzie przetwarzał powierzone dane tylko z wykorzystaniem środków technicznych i organizacyjnych zlokalizowanych na terenie państw należących do Wspólnoty Europejskiej Polski i zarządzanych zgodnie z obowiązującym prawem na jej terenie m.in. Dyrektywą 95/46AA/E Parlamentu Europejskiego i Rady z dnia 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (D.U. L 281 , 23/11/1995).
2. Wykonawca oświadcza, że zestawione połączenia i środki techniczne użyte do tego połączenia będą wykorzystywane tylko i wyłącznie w celu realizacji umów tzn. serwisowania urządzeń objętych umową o wskazanych przez Zamawiającego adresach IP w wydzielonych przez Zamawiającego podsieciach VLAN.
3. Wszystkie połączenia i transmisja danych będzie się odbywała za pośrednictwem bezpiecznego połączenia VPN na statyczny nr IP należący do. Połączenie będzie szyfrowane w sposób bezpieczny.

§ 6

1. Wykonawca oświadcza, że będzie się stosował się do zasad określonych w ust. 2.
2. Wykonawca nie może:
   a) zmieniać przyznanych adresów IP,
   b) rozdzielać sygnału na inne urządzenia niż określony w umowie (np. stosowanie routera itp.),
   c) samowolnie dokonywać jakichkolwiek zmian w infrastrukturze telekomunikacyjnej,
   d) dokonywać przeciążenia sieci telekomunikacyjnej,
   e) rozsyłać niechcianej poczty (SPAM),
   f) używać niedozwolonych narzędzi sieciowych, takich jak sniffery, skanery portów, exploity,
   g) wykorzystywać infrastruktury telekomunikacyjnej w celu uruchamiania serwisów świadczących usługi komercyjne,
   h) rozpowszechniać informacji sprzecznych z obowiązującym prawem oraz naruszających w jakikolwiek sposób uczucia religijne lub normy społeczne i obyczajowe,
   i) świadczyć usług telekomunikacyjnych osobom trzecim, o ile wiążą się one z tranzytem informacji przez sieć Szpitala,
   j) prowadzić jakichkolwiek działań, które mogą powodować zakłócenia w działaniu sieci,
   k) podejmować jakichkolwiek działań, które mogą uszkodzić infrastrukturę telekomunikacyjną, za pomocą której świadczona jest usługa lub mogących zakłócić poprawne funkcjonowanie systemów służących udostępnianiu i monitorowaniu usługi oraz urządzeń i łączy przeznaczonych do przekazywania informacji na odległość, za pomocą których świadczona jest Usługa,
   l) dokonywać nieuzgodnionych z Zamawiającym napraw i zmian (w tym również instalacji oprogramowania i urządzeń sieciowych) w infrastrukturze telekomunikacyjnej Szpitala,
   m) stosować urządzeń sieciowych i oprogramowania niedozwolonych przez prawo,
   n) kierować do sieci Szpitala ruch telekomunikacyjny z innych sieci telekomunikacyjnych bez zgody Szpitala,
   o) odmówić dostępu do infrastruktury telekomunikacyjnej Szpitala, w celu ich kontroli, konserwacji lub naprawy,

Zasady powierzenia przetwarzania danych osobowych

p) wykorzystywać urządzeń udostępnionych przez Szpital lub inne przyłączone do punktu styku z siecią publiczną Internet , niezgodnie z przepisami prawa lub niezgodnie z zawartą umową,
q) uzyskiwać ani próbować uzyskiwać żadnych informacji z sieci Szpitala przy użyciu jakiejkolwiek metody, która nie została wyraźnie dopuszczona przez Szpital,
r) przechwytywać, badać lub w inny sposób analizować jakiegokolwiek komunikacyjnego protokołu używanego przez Szpital, zarówno poprzez analizator sieci, program przechwytujący (sniffer) lub inne urządzenie.
s) podejmować działań, które nie są niezbędne do realizacji zawartych z Zamawiającym umów.

Oświadczenie o zachowaniu poufności

Ja, niżej podpisany .....
/Imiona, nazwisko, nr PESEL/

będący pracownikiem firmy ..... z siedzibą w ..... ul. ..... zwanej dalej „Wykonawcą", z którą Szpital zawarł umowę nr 155/ZP/15

Ja, niżej podpisany, niniejszym oświadczam, że posiadam upoważnienie do przetwarzania danych osobowych, zapoznałem się z przepisami dotyczącymi ochrony danych osobowych i zobowiązuję się do przestrzegania:

1. Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.z 2014 poz. 1182 z późn.zm.)).
2. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

niniejszym zobowiązuję się do

- Wykonywania prac wdrożeniowych/serwisowych zgodnie z postanowieniami umowy,
- zachowania w tajemnicy, w trakcie trwania umowy oraz po jej ustaniu wszelkich informacji dotyczących funkcjonowania systemów i urządzeń w Szpitalu tzn. informacji technicznych, technologicznych, prawnych organizacyjnych dotyczących urządzeń, systemów informatycznych/teleinformatycznych (np. urządzenia, wyroby medyczne, sprzęt informatyczny), uzyskanych w trakcie realizacji umowy niezależnie od formy i źródła ich pozyskania, zachowania w tajemnicy uzyskanych haseł dostępu do systemów informatycznych i urządzeń medycznych, pomieszczeń itp.,
- w przypadku dostępu do danych osobowych przetwarzanych w Szpitalu zachowania bezterminowo w tajemnicy tych danych niezależnie od sposobu ich pozyskania i przetwarzania a także nieudostępniania tych danych osobom trzecim,
- wykorzystania w/w informacji jedynie w celach określonych w umowie,
- zapewnienia bezpieczeństwa pozyskanych informacji w szczególności danych osobowych tzn. zapewnienia ochrony przed dostępem osób nieupoważnionych, uszkodzeniem tych danych, nieuprawnioną ich modyfikacją, niezależnie od nośnika na jakim się znajdują (urządzenia, pamięci masowe, papier, klisza itp.),
- nie wynoszenia poza teren Szpitala jakichkolwiek dokumentów/nośników informacji, jak również ich kopii sporządzonych w jakiejkolwiek formie w szczególności zawierających dane osobowe,
- **nie sporządzania jakichkolwiek kopii dokumentów/plików (niezależnie od nośnika) zawierających informacje dotyczące Szpitala lub jego pacjentów z wyłączeniem wykonywanych kopi bezpieczeństwa na zasobach będących własnością Zamawiającego,**
- **nie wykorzystywania, nie będących własnością Szpitala nośników danych (np. urządzenia pamięci masowej, kamery, aparaty, telefony komórkowe, komputery) do utrwalania: danych, plików, zdjęć, filmów, dokumentów, zdarzeń na terenie Szpitala**
- natychmiastowego zgłaszania osobie nadzorującej umowę oraz Administratorowi Bezpieczeństwa Informacji w Szpitalu próby lub faktu naruszenia zabezpieczenia pomieszczenia, bezpieczeństwa zbioru danych osobowych, urządzenia lub systemu informatycznego, w którym przetwarzane są dane osobowe,

Powyższe oświadczenie potwierdzam własnym podpisem

....., dnia ..... *Miejscowość*

..... *czytelny podpis osoby składającej oświadczenie*

Oświadczenie o zachowaniu poufności

Instrukcja wykonywania kopii bezpieczeństwa danych zawartych w systemie ARIA WSS im. M. Kopernika w Łodzi

1. Przed przystąpieniem do czynności serwisowych, które mogą spowodować naruszenie integralności danych zawartych w systemie „ARIA" uprawniony inżynier serwisu jest zobowiązany do wykonania kopii bezpieczeństwa.
2. Kopie danych wykonywane są na udostępnionych zasobach będących własnością WSS im. M. Kopernika w Łodzi lub na dyskach będących własnością „Candeli" i dedykowanych do wykonywania kopii bezpieczeństwa.
3. „Candela" prowadzi ewidencję przeznaczonych do wykonywania kopii bezpieczeństwa dysków.
4. Pracownicy/ współpracownicy „Candeli" zobowiązani są do zabezpieczenia dysków przed zagubieniem i nieuprawnionym dostępem.
5. Dyski wykorzystywane do wykonywania kopii bezpieczeństwa muszą być zaszyfrowane Do szyfrowania należy używać algorytmów ogólnie uznanych za silne tj. dla kluczy symetrycznych AES (128 bit) lub 3DES, a dla kluczy asymetrycznych klucz długości minimum 1024 bit. Klucze zostaną udostępnione tylko uprawnionym inżynierom serwisu.
6. Po zakończeniu czynności serwisowych i sprawdzeniu integralności danych zawartych w systemie „ARIA" w przypadku braku konieczności odtworzenia danych z kopii bezpieczeństwa inżynier serwisu zobowiązany jest do trwałego usunięcia kopii bezpieczeństwa z dysku w taki sposób by nie można było odtworzyć tych danych.
7. Każda czynność wykonania i usunięcia kopii bezpieczeństwa z dysków będących własnością „Candeli" zostanie odnotowana w raporcie z czynności serwisowych, w którym zostanie potwierdzone przez inżyniera serwisu trwałe usunięcie danych z tych dysków.

Powyższe oświadczenie potwierdzam własnym podpisem

....., dnia .....
Miejscowość

.....
czytelny podpis osoby składającej oświadczenie