WOJEWÓDZKI SZPITAL SPECJALISTYCZNY
WE WROCŁAWIU
51-124 Wrocław, ul. H. Kamieńskiego 73a
telefony: centrala 71 32 70 100, fax 71 32 54 101
www.wssk.wroc.pl

Wrocław, dn. 20.08.2014 r.

Znak postępowania: Szp/FZ – 44/2014

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA
(SIWZ)

Postępowanie o udzielenie zamówienia publicznego
w trybie przetargu nieograniczonego
prowadzonego
przez Wojewódzki Szpital Specjalistyczny we Wrocławiu
z siedzibą we Wrocławiu przy ul. H. Kamieńskiego 73a
zgodnie z art. 39 Ustawy Prawo Zamówień Publicznych.

DOSTAWA ZINTEGROWANEGO SYSTEMU BEZPIECZEŃSTWA SIECI UTM

Z UPOWAŻNIENIA DYREKTORA
Z-ca DYREKTORA
ds. Finansów i Administracji
mgr inż. Jadwiga Raziuk

Radca prawny
Iwona Jakubiak
.....
Sprawdzono pod względem prawnym

.....
Zatwierdzam

ROZDZIAŁ I
INFORMACJE OGÓLNE

1. Zamawiającym jest:
   Wojewódzki Szpital Specjalistyczny we Wrocławiu, ul. H. Kamieńskiego 73A, 51-124 Wrocław
   adres do korespondencji:
   Wojewódzki Szpital Specjalistyczny we Wrocławiu
   Dział Zaopatrzenia i Zamówień Publicznych
   ul. H. Kamieńskiego 73A, 51-124 Wrocław
2. Ogłoszenie o zamówieniu zostanie zamieszczone na stronie internetowej Zamawiającego oraz na tablicy ogłoszeń w siedzibie Wojewódzkiego Szpitala Specjalistycznego we Wrocławiu od dnia zamieszczenia ogłoszenia o zamówieniu w Biuletynie Zamówień Publicznych do upływu terminu składania ofert.
3. Godziny urzędowania Zamawiającego: od poniedziałku do piątku od godz. 7:30 do 14:35.
4. Jako podstawowy dokument do sporządzenia oferty należy traktować niniejszą SIWZ.
5. Do czynności podejmowanych przez Zamawiającego i Wykonawcę stosować się będzie przepisy ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2014 r., poz. 121), jeżeli przepisy ustawy Pzp nie stanowią inaczej.

ROZDZIAŁ II
TRYB UDZIELENIA ZAMÓWIENIA

1. Postępowanie prowadzone jest w trybie przetargu nieograniczonego przy wartości zamówienia poniżej 207 000,00 euro.
2. Podstawa prawna opracowania specyfikacji istotnych warunków zamówienia:
   1) Ustawa z dnia 29 stycznia 2004 r. Prawo Zamówień Publicznych (Dz. U. z 2013 r. poz. 907 ze zm.), zwana dalej Pzp,
   2) Rozporządzenie Prezesa Rady Ministrów z dnia 19 lutego 2013 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy, oraz form, w jakich te dokumenty mogą być składane (Dz. U. z 2013 r. poz. 231),
   3) Rozporządzenie Prezesa Rady Ministrów z dnia 23 grudnia 2013 r. w sprawie średniego kursu złotego w stosunku do euro stanowiącego podstawę przeliczania wartości zamówień publicznych (Dz. U. z 2013 r. poz. 1692),
   4) Rozporządzenie Prezesa Rady Ministrów z dnia 23 grudnia 2013 r. w sprawie kwot wartości zamówień oraz konkursów, od których jest uzależniony obowiązek przekazywania ogłoszeń Urzędowi Publikacji Unii Europejskiej (Dz. U. z 2013 r. poz. 1735),
   5) Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 ze zm.)

ROZDZIAŁ III
OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest dostawa zintegrowanego systemu bezpieczeństwa sieci UTM dla potrzeb Zamawiającego, którego szczegółowy opis zawiera załącznik nr 8 do SIWZ zwanego dalej „Systemem".
2. Przedmiot zamówienia obejmuje:
   1) dostawę, zainstalowanie, uruchomienie i przetestowanie fabrycznie nowego i nieużywanego zintegrowanego systemu bezpieczeństwa sieci UTM, zgodnie z wymaganymi parametrami techniczno – użytkowymi stanowiącym zał. nr 9 do SIWZ,
   2) dostawę licencji aktywacyjnych dla funkcji bezpieczeństwa na okres 36 miesięcy,
   3) Wykonanie infrastruktury informatycznej zawierającej:

a) przygotowanie projektu infrastruktury informatycznej oraz planu wdrożenia zgodnie z wytycznymi Zamawiającego,
b) zainstalowanie, uruchomienie oraz implementacja planu wdrożenia infrastruktury informatycznej,
c) przeprowadzenie testów działania oraz testów wysokiej dostępności rozwiązania,
d) wykonanie dokumentacji powykonawczej,

4) przeprowadzenie jednodniowego szkolenia stanowiskowego dla 2 administratorów w terminie wskazanym przez Zamawiającego.
5) udzielenie wsparcia technicznego przez okres 36 miesięcy liczone od daty odbioru zintegrowanego systemu bezpieczeństwa sieci UTM, w ramach którego Wykonawca zapewni:
   a) aktualizacje dostarczonego Systemu do nowych wersji oprogramowania, patche, szkolenia administratorów on-site z nowych funkcjonalności,
   b) usługi konsultacyjne w zakresie funkcjonalności, eksploatacji i administrowania Systemem,
   c) bieżące aktualizacje dokumentacji technicznej dla Systemu,
   d) obsługę zgłoszeń problemów dotyczących Systemu poprzez telefon lub e-mail 24 h na dobę 7 dni w tygodniu,

3. Urządzenia centralnego systemu logowania i raportowania FortiAnalyzer, w które obecnie wyposażony jest Zamawiający nadal będą wykorzystywane.
4. Zamawiający wymaga aby dostarczony system bezpieczeństwa sieci UTM był kompatybilny z posiadanym przez Zamawiającego urządzeniami FortiAP, na poziomie zarządzania politykami firewall i reguł bezpieczeństwa.
5. Zaoferowany system bezpieczeństwa sieci UTM musi posiadać możliwość integracji z wykorzystywanym przez Zamawiającego systemem centralnego logowania i raportowania FortiAnalyzer 1000C.
6. Zamawiający w ramach wynagrodzenia umownego wymaga również udzielenia wsparcia technicznego przez okres 36 miesięcy dla posiadanego systemu centralnego logowania i raportowania FortiAnalyzer 1000C, w ramach którego Wykonawca zapewni:
   1) aktualizacje posiadanego systemu logowania i raportowania do nowych wersji oprogramowania, patche, szkolenia administratorów on-site z nowych funkcjonalności,
   2) usługi konsultacyjne w zakresie funkcjonalności, eksploatacji i administrowania Systemem FortiAnalyzer 1000C,
   3) bieżące aktualizacje dokumentacji technicznej dla posiadanego systemu,
   4) obsługę zgłoszeń problemów dotyczących systemu poprzez telefon lub e-mail 24 h na dobę 7 dni w tygodniu,
7. Zamawiający wymaga udzielenia 36 - miesięcznej gwarancji producenta na przedmiot zamówienia o którym mowa w ust. 1 niniejszego rozdziału oraz posiadanych przez Zamawiającego urządzeń FortiAP o których mowa w ust. 4 niniejszego rozdziału, liczonej od daty jego odbioru.
8. W okresie gwarancji Wykonawca w ramach wynagrodzenia umownego zobowiązuje się do:
   1) przeprowadzenia przeglądów serwisowych przedmiotu zamówienia, zgodnie ze wskazaniami producenta, nie rzadziej niż raz na 12 miesięcy, (tzn. minimum trzy przeglądy w okresie trwania gwarancji) przy czym ostatni serwis powinien zostać przeprowadzony najpóźniej 3 miesiące po dacie wygaśnięcia okresu gwarancyjnego,
   2) wymiany elementów zużywalnych, których wymiana wchodzi w zakres okresowej obsługi serwisowej przedmiotu zamówienia,
   3) przyjmowania zgłoszeń serwisowych przez dedykowany serwisowy moduł internetowy oraz infolinię w trybie całodobowym 7 dni w tygodniu.
   4) reakcji serwisu technicznego w ciągu 1 godziny w dni robocze od momentu zgłoszenia awarii Wykonawcy. *„Reakcję serwisu"* rozumie się jako działanie, które ma doprowadzić do usunięcia usterki lub diagnozy uszkodzenia w drodze telefonicznego wywiadu technicznego, serwisu zdalnego lub wizyty osobistej pracownika działu serwisu Wykonawcy,
   5) zakończenia naprawy przedmiotu zamówienia w terminie do 7 dni roboczych od daty zgłoszenia awarii,

6) Zamawiający wymaga dostarczenia na czas naprawy, urządzenia zastępczego o parametrach technicznych takich samych lub wyższych w terminie 8 godzin od daty zgłoszenia awarii urządzenia.
7) wymiany przedmiotu zamówienia na nowy w przypadku 5 awarii powodujących wyłączenie urządzenia z eksploatacji, w okresie jednego roku trwania gwarancji,

9. Zamawiający wymaga również udzielenia 36 - miesięcznej gwarancji producenta dla posiadanych przez Zamawiającego urządzeń FortiAP o których mowa w ust. 4 niniejszego rozdziału, liczonej od daty jego odbioru.
10. W przypadku konieczności wymiany Systemu w okresie gwarancji, gwarancja jest wznawiana.
11. Zamawiający wymaga, aby Wykonawca dołączył do oferty oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzacje producenta w zakresie sprzedaży oferowanego Systemu oraz świadczenia usług z nimi związanych.
12. Zamawiający dopuszcza składanie ofert równoważnych przy zachowaniu norm, parametrów i standardów, jakimi charakteryzuje się opisany przez Zamawiającego przedmiot zamówienia. Zgodnie z art. 30 ust. 5 Ustawy Pzp Wykonawca, który powołuje się na rozwiązania równoważne obowiązany jest wykazać, że oferowane przez niego dostawy spełniają wszystkie parametry graniczne określone w SIWZ.
13. Wskazanie przez Zamawiającego marki lub nazwy handlowej określa klasę produktu, będącego przedmiotem zamówienia i służy ustaleniu standardu, a nie wskazuje na konkretny wyrób lub konkretnego producenta. Oryginalne nazewnictwo lub symbolika podana została w celu prawidłowego określenia przedmiotu zamówienia.
14. Zamawiający ma prawo do sprawdzenia wiarygodności podanych przez Wykonawcę parametrów technicznych we wszystkich dostępnych źródłach, w tym również poprzez zwrócenie się o złożenie dodatkowych wyjaśnień do Wykonawcy.
15. Przedmiot zamówienia i jego elementy muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
16. Kod CPV: 48.00.00.00-8 oprogramowania i systemy informatyczne
72.26.30.00-6 usługi wdrażania oprogramowania

ROZDZIAŁ IV
DODATKOWE INFORMACJE DOTYCZĄCE PRZEDMIOTU ZAMÓWIENIA

1. Zamawiający nie dopuszcza składania ofert częściowych.
2. Zamawiający nie dopuszcza składania ofert wariantowych.
3. Zamawiający nie przewiduje udzielenia zamówień uzupełniających, o których mowa w art. 67 ust. 1 pkt 7) ustawy Pzp.
4. Zamawiający nie przewiduje zawarcia umowy ramowej.
5. Zamawiający nie przewiduje prowadzenia aukcji elektronicznej.

ROZDZIAŁ V
TERMIN WYKONANIA ZAMÓWIENIA

Zamawiający wymaga, aby zamówienie było zrealizowane w ciągu 30 dni od daty podpisania umowy.

ROZDZIAŁ VI
WARUNKI UDZIAŁU W POSTĘPOWANIU, OPIS SPOSOBU DOKONYWANIA OCENY SPEŁNIANIA TYCH WARUNKÓW ORAZ WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW, JAKIE MAJĄ DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIENIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:
1) nie podlegają wykluczeniu z postępowania na podstawie art. 24 uPzp;
2) spełniają warunki udziału w postępowaniu określone w art. 22 uPzp.

2. Wykonawcy muszą złożyć dokumenty lub oświadczenia wymienione w tabeli:

A	W CELU WYKAZANIA BRAKU PODSTAW DO WYKLUCZENIA Z POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA WYKONAWCA SKŁADA NASTĘPUJĄCE DOKUMENTY:	WYMAGANE DOKUMENTY LUB OŚWIADCZENIA 1. Oświadczenia z art. 24 ust. 1 uPzp – Załącznik nr 4 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 uPzp, wystawionego nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
WARUNEK UDZIAŁU W POSTĘPOWANIU		DOKUMENTY LUB OŚWIADCZENIA POTWIERDZAJĄCE SPEŁNIANIE WARUNKU
B	**W celu wykazania spełnienia przez Wykonawcę warunków określonych w art. 22 ust. 1 uPzp**	Oświadczenia z art. 22 ust. 1 uPzp – Załącznik nr 3 do SIWZ
	<u>WIEDZA I DOŚWIADCZENE</u> Warunkiem udziału w postępowaniu jest: - wykazanie się należytym wykonaniem w okresie ostatnich trzech lat przed upływem terminu składania ofert co najmniej 1 zamówieniem odpowiadającym swoim rodzajem przedmiotowi zamówienia o wartości nie mniejszej niż 150 000,00 PLN	1. Wykaz wykonanych, a w przypadku świadczeń okresowych lub ciągłych wykonywanych głównych dostaw w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których zostały wykonane wraz z <u>załączeniem dowodów,</u> czy zostały wykonane lub są wykonywane należycie - załącznik nr 6 do SIWZ.
	<u>DYSPONOWANIE OSOBAMI ZDOLNYMI DO WYKONANIA ZAMÓWIENIA,</u> **tj. wskazanie osób posiadających kwalifikacje zawodowe oraz doświadczenie** 1) co najmniej 3 zatrudnionymi osobami posiadającymi certyfikat Fortinet Certified Network Security Proffesional (FCNSP) lub równoważny w oferowanej technologii 2) co najmniej 1 osobą posiadającą certyfikat Fortinet Troubleshootting Training lub równoważne szkolenie z zakresu wykrywania problemów w oferowanej technologii	2. Wykaz osób, które będą uczestniczyć w wykonywaniu zamówienia, w szczególności odpowiedzialnych za świadczenie usług, kontrolę jakości wraz z informacjami na temat ich kwalifikacji zawodowych, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia, a także zakresu wykonywanych przez nie czynności, oraz informacją o podstawie do dysponowania tymi osobami – zgodnie z załącznikiem nr 6 do SIWZ. 3. Oświadczenie Wykonawcy, że osoby, które będą uczestniczyć w wykonywaniu zamówienia posiadają wymagane uprawnienia np. ukończone szkolenie potwierdzone certyfikatem autoryzowanego producenta proponowanego systemu *(w przypadku posiadania przez wykonawcę certyfikatów w oświadczeniu należy wskazać podmiot wystawiający certyfikat, datę ważności oraz nr certyfikatu)*

<u>Niespełnienie jednego z wymienionych w ust.2 litera A warunków skutkować będzie wykluczeniem Wykonawcy z postępowania i uznaniem jego oferty za odrzuconą. Niespełnienie warunku wymienionego w ust. 2 litera B warunku skutkować będzie odrzuceniem oferty.</u>

3. Wykonawca może polegać na wiedzy i doświadczeniu, innych podmiotów, niezależnie od charakteru prawnego łączących go z nimi stosunków. Wykonawca w takiej sytuacji zobowiązany jest udowodnić Zamawiającemu, iż będzie dysponował zasobami do realizacji zamówienia. W szczególności przedstawiając w tym celu pisemne zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na okres korzystania z nich przy wykonaniu zamówienia.
4. Jeżeli Wykonawca wykazując spełnianie warunków, o których mowa w art. 22 ust. 1 uPzp, polega na zasobach innych podmiotów na zasadach określonych w art. 26 ust. 2b uPzp, a podmioty te będą brały udział w realizacji części zamówienia, Zamawiający żąda od Wykonawcy przedstawienia w odniesieniu do tych podmiotów dokumentów wymienionych w pkt. A niniejszego rozdziału.

5. Jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby Wykonawca powoływał się, na zasadach określonych w art. 26 ust. 2b uPzp, w celu wykazania spełniania warunków udziału w postępowaniu, o których mowa w art. 22 ust. 1 uPzp Wykonawca jest obowiązany wykazać Zamawiającemu, iż proponowany inny podwykonawca lub wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż wymagany w trakcie postępowania o udzielenie zamówienia.
6. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentów, o których mowa w pkt 2.A.2 niniejszego rozdziału, składa dokument lub dokumenty, wystawione w kraju, w którym ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że nie otwarto jego likwidacji ani nie ogłoszono upadłości;
7. Dokumenty, o których mowa w ust 6 powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
8. 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 6 niniejszego rozdziału, zastępuje się je dokumentem zawierającym oświadczenie, w którym określa się także osoby uprawnione do reprezentacji Wykonawcy złożone przed właściwym organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego odpowiednio w kraju miejsca zamieszkania osoby lub kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub przed notariuszem.
9. Dokumenty, o których mowa w ust. 2.A.2 oraz ust. 2.B niniejszego rozdziału są składane w formie oryginału lub kopii poświadczonej za zgodność z oryginałem przez Wykonawcę. W przypadku podmiotów o których mowa w ust. 4 niniejszego rozdziału, kopię dokumentów dotyczących odpowiedniego Wykonawcy lub tych podmiotów są poświadczane za zgodność z oryginałem przez Wykonawcę lub te podmioty. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.

ROZDZIAŁ VII
OFERTA WSPÓLNA

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie niniejszego zamówienia. W przypadku złożenia oferty wspólnej przez kilka podmiotów, każdy z nich zobowiązany jest przedstawić dokumenty wystawione na niego wymienione w rozdziale VI pkt 2.A, natomiast dokumenty wymienione w pkt 2.B rozdziału VI, podmioty składają wspólnie, tj.: warunki w nich określone są spełnione, gdy podmioty składające ofertę spełniają je łącznie.
2. Oferta wspólna musi zostać przygotowana i złożona w następujący sposób:
    1) partnerzy ustanawiają i wskazują Pełnomocnika do reprezentowania ich w postępowaniu o udzielenie niniejszego zamówienia albo reprezentowania w postępowaniu o udzielenie niniejszego zamówienia i zawarcia umowy w sprawie zamówienia publicznego;
    2) oferta musi być podpisana w taki sposób, by prawnie zobowiązywała wszystkich Partnerów;
    3) każdy z Partnerów musi złożyć oświadczenie, że nie podlega wykluczeniu z postępowania na podstawie art. 24 ust. 1 uPzp (Załącznik nr 4) oraz musi złożyć odnoszące się do niego dokumenty, wymienione w pkt 2.A rozdziału VI;
    4) partnerzy Konsorcjum muszą udokumentować, że razem spełniają wymagania art. 22 ust. 1 pkt 1- 4 uPzp;
    5) wszelka korespondencja prowadzona będzie wyłącznie z Pełnomocnikiem.

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

1. Zgodnie z art. 27 ust. 1 i 2 ustawy Pzp wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje kierowane do Zamawiającego składane będą za pośrednictwem faksu lub drogą elektroniczną zarówno przez Zamawiającego jak i Wykonawcę, z zastrzeżeniem ust. 3 niniejszego rozdziału.
2. Zamawiający lub Wykonawca przekazując oświadczenia, wnioski, zawiadomienia oraz informacje faksem lub drogą elektroniczną na żądanie każdej ze stron niezwłocznie potwierdza fakt ich otrzymania.
3. Forma pisemna zastrzeżona jest do złożenia oferty wraz z załącznikami.
4. Zamawiający nie udziela żadnych ustnych i telefonicznych informacji, wyjaśnień czy odpowiedzi na kierowane zapytania.
5. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia. Zamawiający udzieli 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.
6. Jeżeli wniosek o wyjaśnienie treści specyfikacji istotnych warunków zamówienia wpłynął po upływie terminu składania wniosku lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpatrzenia.
7. Wnioski o wyjaśnienie treści SIWZ, sposobu złożenia oferty oraz realizacji zamówienia należy przesłać na numer faxu (71) 32 70 425 lub drogą elektroniczną na adres: zp@wssk.wroc.pl
   Adres do korespondencji listownej:
   Wojewódzki Szpital Specjalistyczny we Wrocławiu
   Dział Zaopatrzenia i Zamówień Publicznych
   ul. Kamieńskiego 73A 51-124 Wrocław
   z dopiskiem: postępowanie nr Szp/FZ – 44/2014
   Osobą uprawnioną do porozumiewania się z Wykonawcami jest Monika Wojciechowska - tel. 71/32 70 591.

ROZDZIAŁ IX
WYMAGANIA DOTYCZĄCE WADIUM

Zamawiający w niniejszym postępowaniu nie wymaga wniesienia wadium.

ROZDZIAŁ X
TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca pozostaje związany złożoną ofertą przez 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
2. Zamawiający zastrzega sobie możliwość co najmniej na 3 dni przed upływem terminu związania ofertą, jednorazowego zwrócenia się do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni.

ROZDZIAŁ XI
OPIS SPOSOBU PRZYGOTOWANIA OFERTY

1. Wymagania podstawowe.
   1) każdy Wykonawca może złożyć tylko jedną ofertę. Złożenie większej liczby ofert lub oferty zawierającej propozycje wariantowe spowoduje odrzucenie wszystkich ofert złożonych przez Wykonawcę,
   2) oferta musi być jednoznaczna i kompleksowa tj. obejmować cały przedmiot zamówienia lub odpowiednio wybrany pakiet,
   3) ofertę należy przygotować ściśle według wymagań określonych w niniejszej SIWZ,

4) oferta musi być podpisana przez osoby upełnomocnione do reprezentowania Wykonawcy i zaciągania w jego imieniu zobowiązań finansowych, w wysokości odpowiadającej cenie oferty. Oznacza to, iż jeżeli z dokumentu określającego status prawny Wykonawcy lub pełnomocnictwa wynika, iż do reprezentowania Wykonawcy upoważnionych jest łącznie kilka osób, dokumenty wchodzące w skład oferty muszą być podpisane przez wszystkie te osoby,
5) pełnomocnictwo osób podpisujących ofertę do reprezentowania Wykonawcy, zaciągania w jego imieniu zobowiązań finansowych w wysokości odpowiadającej cenie oferty oraz podpisania oferty musi bezpośrednio wynikać z dokumentów dołączonych do oferty. Oznacza to, że jeżeli pełnomocnictwo takie nie wynika wprost z dokumentu stwierdzającego status prawny Wykonawcy (odpisu z właściwego rejestru), to do oferty należy dołączyć oryginał lub poświadczoną za zgodność z oryginałem przez notariusza, kopię pełnomocnictwa wystawionego na reprezentanta Wykonawcy przez osoby do tego upełnomocnione,
6) Zamawiający może żądać przedstawienia oryginału lub notarialnie poświadczonej kopii dokumentu wyłącznie wtedy, gdy złożona przez Wykonawcę kopia dokumentu jest nieczytelna lub budzi wątpliwości co do jej prawdziwości,
7) we wszystkich przypadkach, gdzie jest mowa o pieczątkach, Zamawiający dopuszcza złożenie czytelnego podpisu,
8) Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

2. Forma oferty:

1) oferta sporządzona zostanie czytelnie w języku polskim, z zachowaniem formy pisemnej pod rygorem nieważności.
2) Formularz ofertowy Załącznik Nr 1 napisany będzie na komputerze oraz podpisany przez osobę (-y) uprawnioną (-e) na podstawie odrębnych przepisów do składania oświadczeń woli - reprezentowania firmy na zewnątrz wraz z pieczątką (-ami) imienną (-ymi).
3) zaleca się, aby wszystkie zapisane strony oferty były ponumerowane oraz aby wszystkie dokumenty załączone do oferty były parafowane przez osobę (lub osoby, jeżeli do reprezentowania Wykonawcy upoważnione są dwie lub więcej osób) podpisującą (podpisujące) oferty zgodnie z treścią dokumentu określającego status prawny Wykonawcy lub treścią załączonego do oferty pełnomocnictwa.
4) wszelkie miejsca w ofercie, w których Wykonawca naniósł poprawki lub zmiany wpisywanej przez siebie treści muszą być parafowane przez osobę (osoby) podpisującą (podpisujące) ofertę.
5) wszelkie dokumenty i oświadczenia w językach obcych należy złożyć wraz z tłumaczeniem na język polski, poświadczonym przez Wykonawcę.
6) dla uznania ważności oferta musi zawierać wszystkie wymagane w SIWZ aktualne dokumenty – oryginały lub czytelne kopie, poświadczone za zgodność z oryginałami przez osobę (-y) uprawnioną (-e) do reprezentowania firmy na zewnątrz – podpisującą (-e) Ofertę - wraz z podpisem i pieczątką (-ami) imienną (-ymi) podpisującego (-ych).
7) Kopia dokumentu wymaga zapisu *„za zgodność z oryginałem"*.

3. Zawartość oferty.

1) Oferta musi się składać z:
   a) dokumentów i oświadczeń wymienionych w rozdziale VI SIWZ,
   b) formularza ofertowego Wykonawcy - załącznik nr 1 do SIWZ,
   c) informacji o przynależności do tej samej grupy kapitałowej – załącznik nr 5 do SIWZ,
   d) wypełnionego formularza parametrów techniczno - użytkowych (załącznik Nr 9)

Zaleca się, aby Formularz ofertowy wraz z załącznikami (wszystkie wymagane niniejszą SIWZ dokumenty) był zszyty lub spięty w sposób utrudniający jego zdekompletowanie.

4. Informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.
   1) Oferty są jawne od chwili ich otwarcia.

5. W związku z powyższym Wykonawca zobowiązany jest do wypełnienia odpowiedniego punktu wzoru formularza ofertowego. Zastrzeżone informacje winny być odpowiednio oznaczone na właściwym dokumencie widocznym napisem: *„tajemnica przedsiębiorstwa"* i złożone w odrębnej kopercie wewnętrznej, a na ich miejscu w dokumentacji należy zamieścić stosowne odsyłacze.

ROZDZIAŁ XII
MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT

1. Ofertę wraz z wymaganymi dokumentami jw. **należy złożyć w zamkniętej kopercie** oznaczonej **danymi Wykonawcy.** Na kopercie należy umieścić informacje:

nazwa i adres Wykonawcy OFERTA PRZETARGOWA **„Dostawa zintegrowanego systemu bezpieczeństwa sieci UTM"** Uwaga: Nie otwierać przed dniem **04.09.2014 r. godz.10:00** Oferta zawiera ..... kart – ilość kart zastrzeżonych .....

2. Ofertę, sporządzoną zgodnie z wymaganiami niniejszej SIWZ, należy przesłać lub złożyć w Dziale Zaopatrzenia i Zamówień Publicznych Wojewódzkiego Szpitala Specjalistycznego we Wrocławiu przy ul. Kamieńskiego 73a, Budynek nr 10 **do godziny 09:00 do dnia 04.09.2014 r.**
3. Celem dokonania zmian bądź poprawek Wykonawca może wycofać wcześniej złożoną ofertę i złożyć ją po modyfikacji ponownie, pod warunkiem zachowania wyznaczonego w SIWZ terminu składania ofert.
4. Powiadomienie o wprowadzeniu zmian lub wycofaniu oferty powinno zostać złożone w sposób i formie przewidzianej dla oferty z tym, że koperta powinna być dodatkowo opisana *„zmiana"* lub *„wycofanie"*.
5. Po upływie terminu składania ofert Wykonawca nie może dokonać zmian w ofercie.
6. W przypadku nieprawidłowego zaadresowania lub zamknięcia oferty Zamawiający nie bierze odpowiedzialności za złe skierowanie przesyłki i jej przedterminowe otwarcie.
7. Oferty złożone po wyznaczonym terminie zwraca się niezwłocznie, bez ich otwierania.
8. Z zawartością ofert nie można zapoznać się przed upływem terminu otwarcia ofert.
9. Publiczne otwarcie ofert nastąpi w dniu **04.09.2014 r. o godz. 10:00** w Sali audiowizualnej w siedzibie Wojewódzkiego Szpitala Specjalistycznego we Wrocławiu przy ul. Kamieńskiego 73a.
10. W części jawnej, przy udziale osób zainteresowanych, nastąpi:
    - podanie przez Zamawiającego kwoty, jaką zamierza przeznaczyć na sfinansowanie zamówienia,
    - zbadanie nienaruszalności ofert,
    - otwarcie ofert w kolejności ich złożenia,
    - ogłoszenie nazwy i adresy Wykonawców, których oferta jest otwierana oraz ceny ofertowej.
11. Informacje, o których mowa w art. 86 ust. 3 i 4 uPzp Zamawiający prześle Wykonawcom, którzy nie byli obecni na otwarciu ofert, na ich pisemny wniosek.
12. W dalszej niejawnej części Zamawiający zbada ważność ofert, spełnienie warunków wymaganych od Wykonawców oraz dokona ich oceny w oparciu o przyjęte kryterium.
13. Zamawiający informuje, że zgodnie z art. 96 ust. 3 uPzp oferty składane w postępowaniu o udzielenie zamówienia publicznego są jawne i podlegają udostępnieniu od chwili ich otwarcia, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeśli Wykonawca zastrzegł nie później niż w terminie składania ofert, że nie mogą one być udostępniane.

13. Zamawiający informuje, że zgodnie z art. 96 ust. 3 uPzp oferty składane w postępowaniu o udzielenie zamówienia publicznego są jawne i podlegają udostępnieniu od chwili ich otwarcia, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeśli Wykonawca zastrzegł nie później niż w terminie składania ofert, że nie mogą one być udostępniane.

ROZDZIAŁ XIII
OPIS SPOSOBU OBLICZENIA CENY

1. Ceną oferty jest wartość brutto przedmiotu zamówienia.
2. Cenę oferty należy podać w PLN wraz z właściwym podatkiem VAT, z zaokrągleniem do dwóch miejsc po przecinku.
   UWAGA: *Zaokrąglenia cen w złotych należy dokonać do dwóch miejsc po przecinku według zasady, że trzecia cyfra po przecinku od 5 w górę powoduje zaokrąglenie drugiej cyfry po przecinku w górę o 1. Jeżeli trzecia cyfra po przecinku jest niższa od 5, to druga cyfra po przecinku nie ulega zmianie.*
3. Sposób zapłaty i rozliczenia za realizację niniejszego zamówienia, określone zostały w projekcie umowy stanowiący załącznik nr 2 do SIWZ.
4. Cena musi zawierać wszystkie koszty związane z realizacją przedmiotu zamówienia zawarte w formularzu asortymentowo – cenowym stanowiącym załącznik nr 1.1 do SIWZ.
5. Wartość brutto należy liczyć w sposób następujący:
   cena jednostkowa netto x ilość = wartość netto + podatek VAT = wartość brutto
6. Podana cena oferty netto, zamieszczona w „Formularzu ofertowym" (załącznik nr 1 do SIWZ) będzie niezmienna przez cały okres obowiązywania umowy na realizację przedmiotowego zamówienia.
7. Zamawiający nie przewiduje rozliczenia w walutach obcych.

ROZDZIAŁ XIV
POPRAWIANIE OMYŁEK W TREŚCI OFERTY

1. Zamawiający poprawi w tekście oferty:
   1) oczywiste omyłki pisarskie;
   2) oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek;
   3) inne omyłki polegające na niezgodności oferty ze specyfikacją istotnych warunków zamówienia, nie powodujące istotnych zmian w treści oferty

   - niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.
2. Przez „oczywistą omyłkę rachunkową" Zamawiający rozumie omyłkę w przeprowadzeniu rachunków na liczbach, dotyczącą obliczenia ceny, przy czym musi mieć ona charakter oczywisty. Jeżeli charakter omyłki i okoliczności jej popełnienia wskazują, iż każdy racjonalnie działający Wykonawca, który składa ofertę z zamiarem uzyskania zamówienia publicznego, złożyłby ofertę o odmiennej (poprawnej) treści Zamawiający uzna, iż omyłka ma charakter „oczywisty". Jako dopuszczalne oczywiste omyłki rachunkowe Zamawiający uzna:
   1) błędne obliczenie kwoty prawidłowo podanej w kalkulacji cenowej stawki podatku od towarów i usług;
   2) błędne zsumowanie w kalkulacji cenowej wartości: netto, VAT, brutto.
   3) inne omyłki polegające na niezgodności oferty ze specyfikacją istotnych warunków zamówienia, nie powodujące istotnych zmian w treści oferty
3. Za omyłkę określoną w punkcie 2 c) Zamawiający uzna m. in. sytuację, w której cena brutto podana słownie nie odpowiada cenie brutto podanej liczbą. Zamawiający przyjmie za właściwą, cenę obliczoną prawidłowo, wynikającą z sumowania wartości netto i podatku VAT.

ROZDZIAŁ XV
OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY WRAZ Z PODANIEM ZNACZENIA TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

1. Po stwierdzeniu ważności ofert oraz spełnieniu wymagań niniejszej SIWZ, Komisja Przetargowa Zamawiającego dokona oceny merytorycznej ofert w oparciu o kryteria, o których mowa poniżej.

   Kryteria oceny i ich waga.
2. Oferowana cena ogółem brutto za przedmiot zamówienia - 100 %
3. Sposób obliczania wartości punktowej kryterium ceny:

   Wartość punktowa ceny wyliczana będzie według wzoru: $(C_{min} : C_n) \times 100$

   gdzie:

   C_{min} - najniższa cena ogółem brutto spośród ofert nie odrzuconych

   C_n - cena ogółem brutto ocenianej oferty

   gdzie 1 % = 1 pkt
4. W toku dokonywania badania i oceny ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień treści złożonych przez nich ofert.
5. Za ofertę najkorzystniejszą Zamawiający uzna ofertę z największą ilością punktów.

ROZDZIAŁ XVI
INFORMACJE O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAC DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

1. Przy dokonywaniu wyboru oferty najkorzystniejszej Zamawiający stosował będzie wyłącznie zasady i kryteria określone w SIWZ.
2. Zamawiający udzieli zamówienia Wykonawcy, którego oferta zostanie uznana za najkorzystniejszą.
3. O wyborze oferty Zamawiający zawiadomi niezwłocznie Wykonawców zgodnie z art. 92 uPzp.
4. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający zamieści informacje, o których mowa w art. 92 ust. 1 pkt 1) uPzp, również na stronie internetowej oraz w miejscu publicznie dostępnym w swojej siedzibie.
5. W przypadku, gdyby wyłoniona w prowadzonym postępowaniu oferta została złożona przez dwóch lub więcej Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, Zamawiający może zażądać umowy regulującej współpracę tych podmiotów przed przystąpieniem do podpisania umowy o udzielenie zamówienia publicznego.
6. Zamawiający zawrze umowę z wybranym Wykonawcą w terminie nie krótszym niż 5 dni od dnia przekazania zawiadomienia o wyborze oferty, nie później jednak niż przed upływem terminu związania ofertą, z zastrzeżeniem art. 94 ust.2 pkt 1) lit. a) ustawy Pzp.
7. Wybrany Wykonawca zostanie wezwany przez Zamawiającego do podpisania umowy zgodnej z projektem umowy, załączonym do specyfikacji istotnych warunków zamówienia (załącznik nr 2 do SIWZ).
8. Ogłoszenie o udzieleniu zamówienia zamieszczone zostanie w Biuletynie Zamówień Publicznych.

ROZDZIAŁ XVII
WYMAGANIA DOTYCZACE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Zamawiający w niniejszym postępowaniu nie wymaga od Wykonawcy wniesienia zabezpieczenia należytego wykonania umowy.

ROZDZIAŁ XVIII
PROJEKT UMOWY

1. Jako odrębny załącznik nr 2 do SIWZ, Zamawiający zamieścił projekt umowy, która określa warunki umowne realizacji przedmiotowego zamówienia publicznego.
2. Na podstawie art. 144 uPzp, Zamawiający przewiduje możliwość dokonania zmian postanowień zawartej umowy w stosunku do treści oferty na podstawie, której dokonano wyboru Wykonawcy oraz określa warunki tych zmian przez wprowadzenie do zawartej umowy w szczególności aneks dotyczący zmiany terminu realizacji przedmiotu zamówienia w przypadku wystąpienia zmian organizacyjnych leżących po stronie Zamawiającego.
3. Jeżeli Wykonawca, którego oferta zostanie wybrana, uchyla się od zawarcia umowy w sprawie zamówienia publicznego, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert bez przeprowadzania ich ponownego badania i oceny.

ROZDZIAŁ XIX
ŚRODKI OCHRONY PRAWNEJ

1. Wykonawcy, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy, przysługują środki ochrony prawnej określone w dziale VI uPzp, z zastrzeżeniem punktu 3 SIWZ.
2. Środki ochrony prawnej wobec ogłoszenia o zamówieniu oraz specyfikacji istotnych warunków zamówienia przysługują również organizacjom wpisanym na listę organizacji uprawnionych do ich wnoszenia prowadzonej przez Prezesa Urzędu.
3. Odwołanie przysługuje wyłącznie wobec czynności:
   1) opisu sposobu dokonywania oceny spełniania warunków udziału w postępowaniu,
   2) wykluczenia odwołującego z postępowania o udzielenie zamówienia,
   3) odrzucenie oferty odwołującego.
4. Odwołanie powinno wskazywać czynność lub zaniechanie czynności Zamawiającego, której zarzuca się niezgodność z przepisami ustawy, zawierać zwięzłe przedstawienie zarzutów, określać żądania oraz wskazywać okoliczności faktyczne i prawne uzasadniające wniesienie odwołania.
5. Odwołanie wnosi się do Prezesa Izby w formie pisemnej albo elektronicznej opatrzonej bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu w terminie 5 dni :
   1) od dnia przesłania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia,
   2) od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub specyfikacji istotnych warunków zamówienia na stronie internetowej,
   3) od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.
6. Odwołujący przesyła kopię odwołania Zamawiającemu przed upływem terminu do wniesienia odwołania.
7. Zamawiający prześle niezwłocznie, nie później niż w terminie 2 dni od daty otrzymania, kopię odwołania innym Wykonawcom uczestniczącym w postępowaniu o udzielenie zamówienia, a jeżeli odwołanie dotyczy treści ogłoszenia o zamówieniu lub postanowień siwz, zamieści ją na stronie internetowej wzywając Wykonawców do przystąpienia do postępowania odwoławczego.
8. Wykonawca może zgłosić przystąpienie do postępowania odwoławczego w terminie 3 dni od dnia otrzymania kopii odwołania, wskazując stronę, do której przystępuje i interes w uzyskaniu rozstrzygnięcia na korzyść strony, do której przystępuje. Zgłoszenie przystąpienia doręcza się Prezesowi Izby w formie pisemnej albo elektronicznej opatrzonej bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu, a jego kopię przesyła się Zamawiającemu oraz Wykonawcy wnoszącemu odwołanie.

9. Wykonawcy, którzy przystąpili do postępowania odwoławczego, stają się uczestnikami postępowania odwoławczego, jeżeli mają interes w tym, aby odwołanie zostało rozstrzygnięte na korzyść jednej ze stron.
10. Zamawiający lub odwołujący może zgłosić opozycję przeciw przystąpieniu innego Wykonawcy nie później niż do czasu otwarcia rozprawy.
11. Odwołujący oraz wykonawca wezwany zgodnie z ust. 7 nie mogą następnie korzystać ze środków ochrony prawnej wobec czynności Zamawiającego wykonanych zgodnie z wyrokiem Izby lub sądu albo na podstawie art. 186 ust. 2 i 3 uPzp.
12. Na orzeczenie Izby stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.

Załączniki do SIWZ:

Załącznik nr 1 – Formularz Ofertowy
Załącznik nr 1.1 – Formularz asortymentowo - cenowy
Załącznik nr 2 – Projekt umowy
Załącznik nr 3 – Oświadczenie Wykonawcy z art. 22 uPzp
Załącznik nr 4 – Oświadczenie Wykonawcy z art. 24 uPzp
Załącznik nr 5 – Informacja o przynależności do tej samej grupy kapitałowej
Załącznik nr 6 – wykaz osób i podmiotów, które będą uczestniczyć w wykonywaniu zamówienia
Załącznik nr 7 – wykaz głównych dostaw
Załącznik nr 8 – szczegółowy opis przedmiotu zamówienia
Załącznik nr 9 – wymagane minimalne parametry techniczno - użytkowe

Załącznik nr 1 do SIWZ
Nr sprawy Szp/FZ – 44/2014

....., dn. .....
miejscowość

Zamawiający:
Wojewódzki Szpital Specjalistyczny we Wrocławiu
ul. H. Kamieńskiego 73a
51-124 Wrocław

FORMULARZ OFERTOWY

I. DANE WYKONAWCY

1. Nazwa Wykonawcy: ***(Pełnomocnika w przypadku Konsorcjum)***

.....

2. Siedziba Wykonawcy:

ul: .....*kod:* ..... *miejscowość:* .....

3. Adres do korespondencji:

ul: .....*kod:* ..... *miejscowość:* .....

4. NIP: .....
5. REGON: .....
6. TEL: .....
7. FAX:.....
8. MAIL: .....
9. OSOBA DO KONTAKTÓW: .....
10. TEL.: .....

Konsorcjum z ***(jeżeli dotyczy):***

A) Nazwa Partnera: .....

B) Siedziba Partnera: .....

ul: ..... *kod:* ..... *miejscowość:* .....

II. PRZEDMIOT ZAMÓWIENIA

Składam ofertę na zamówienie publiczne nr Szp/FZ – 44/2014 prowadzone w trybie przetargu nieograniczonego pn.: **„Dostawa zintegrowanego systemu bezpieczeństwa sieci UTM"**

III. CENA

Wartość za wykonanie przedmiotu zamówienia wynosi:

Cena netto .....*zł*
VAT .....*% =* .....*zł*
Cena brutto .....*zł*
Słownie: .....
Na oferowane urządzenie udzielam 36 miesięcznej gwarancji liczonej od daty odbioru

Podatek VAT został doliczony do ceny netto zgodnie z obowiązującymi przepisami o podatkach.

IV. POTWIERDZENIE SPEŁNIENIA WYMOGÓW ZAMAWIAJĄCEGO

1. Oświadczam, że zapoznałem się z warunkami zawartymi w SIWZ, ze wszystkimi załącznikami do SIWZ, akceptuje je bez zastrzeżeń oraz uzyskałem informacje konieczne do przygotowania oferty.
2. Zobowiązuję się w przypadku przyznania zamówienia do zawarcia umowy na warunkach określonych w projekcie umowy.
3. Oświadczam, że zaoferowany produkt jest dopuszczony do obrotu i używania na terytorium Rzeczypospolitej Polskiej i na potwierdzenie powyższego posiadam ważne dokumenty zgodnie z obowiązującym prawem.
4. Wszystkie wymagane w niniejszym postępowaniu przetargowym oświadczenia złożyłem ze świadomością odpowiedzialności karnej za składanie fałszywych oświadczeń w celu uzyskania korzyści majątkowych.
5. Zgłoszenie usterek i wad będzie dokonywane przez Zamawiającego faxem wysyłanym na adres serwisu gwarancyjnego znajdującego się w .....tel..... fax .....
6. Osobą odpowiedzialną za realizację przedmiotu zamówienia ze strony Wykonawcy będzie: .....

V. PODWYKONAWCY (wypełnić, jeżeli dotyczy)

*)Dostawy objęte przedmiotowym zamówieniem zamierzam wykonać samodzielnie/wykonać przy udziale podwykonawców.

**)Przy realizacji przedmiotu zamówienia zobowiązuje się do zawarcia umowy z podwykonawcami: .....w zakresie .....

**) wybrać odpowiednio*
***) w przypadku powierzenia wykonania części zamówienia przy udziale podwykonawców*

VI. TAJEMNICA PRZEDSIĘBIORSTWA

KORZYSTAJĄC z uprawnienia nadanego treścią art. 8 ust. 3 ustawy Prawo zamówień publicznych z dnia 29.01.2004 r. zastrzegam, że informacje:

.....

(wymienić czego dotyczy)
zawarte są w następujących dokumentach:

.....

stanowią tajemnicę przedsiębiorstwa zgodnie z definicją zawartą w treści art. 11 ust. 4 ustawy z 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji,. *(Dz. U. z 2003 roku. nr 153, poz. 1503 z późn. zm.)* i nie mogą być udostępniane innym uczestnikom postępowania.

Na potwierdzenie spełnienia wymagań do niniejszej oferty załączam:.

.....

.....

Na ..... kolejno ponumerowanych stronach składam całość oferty.

.....

(podpis i pieczątka imienna osoby
uprawnionej do reprezentowania Wykonawcy)

Załącznik nr 1.1. do oferty

.....
pieczątka Wykonawcy

nr Szp/FZ – 44/2014

Formularz asortymentowo cenowy

Nazwa przedmiotu zamówienia	Typ/ producent	jedn. miary	Ilość	cena jednostkowa netto	wartość netto	VAT %	cena jednostkowa brutto	wartość brutto
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
*)								
							RAZEM	

wartość brutto słownie: .....

***) Zamawiający wymaga, aby Wykonawca dołączył do oferty oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzacje producenta w zakresie sprzedaży oferowanego Systemu oraz świadczenia usług z nimi związanych**

***) wpisać wszystkie elementy podlegające wycenie**

Wykonawca

.....
(podpis i pieczątka imienna osoby uprawnionej do reprezentowania Wykonawcy)

Załącznik nr 2 do SIWZ
Nr sprawy Szp/FZ – 44/2014

UMOWA - PROJEKT

W dniu ..... we Wrocławiu, pomiędzy Wojewódzkim Szpitalem Specjalistycznym we Wrocławiu z siedzibą we Wrocławiu przy ul. Kamieńskiego 73a działającym na podstawie wpisu do KRS nr 0000101546 w Sądzie Rejonowym dla Wrocławia – Fabrycznej we Wrocławiu, VI Wydział Gospodarczy Krajowego Rejestru Sądowego NIP 895-16-45-574, REGON 000977893, reprezentowanym przez:

prof. dr hab. Wojciecha Witkiewicza - Dyrektora

zwanym dalej „Zamawiający"

a:
..... –
prowadzącą działalność na podstawie..... NIP ....., REGON .....
reprezentowanym przez:
.....
.....
zwanym dalej „Wykonawca"
została zawarta umowa o następującej treści :

§ 1
PRZEDMIOT UMOWY

W wyniku przeprowadzonej procedury przetargowej w trybie przetargu nieograniczonego (sygnatura sprawy Szp/FZ – 44/2014) zgodnie z Ustawą Prawo Zamówień Publicznych Wykonawca zobowiązuje się do dostawy, zainstalowania, uruchomienia i przetestowania zintegrowanego systemu bezpieczeństwa sieci UTM dla potrzeb Zamawiającego zgodnie z ofertą będącą załącznikiem nr 1 do umowy.

§ 2
TERMIN I WARUNKI DOSTAWY

1. Wykonawca zrealizuje przedmiot umowy w terminie 30 dni od daty podpisania umowy.
2. Wykonawca zgłosi Zamawiającemu, z minimum 5 dniowym wyprzedzeniem, gotowość realizacji przedmiotu umowy.
3. Wykonawca dostarczy przedmiot umowy z dokumentacją obsługi w języku polskim.
4. Dostawa poszczególnych elementów zintegrowanego systemu bezpieczeństwa sieci UTM zostanie potwierdzona protokołem odbioru częściowego. Podpisanie protokołu odbioru częściowego nie jest równoznaczne ze stwierdzeniem kompletności i prawidłowości instalacji systemu.
5. Wykonawca sporządzi w obecności Zamawiającego końcowy protokół odbioru prac, obejmujący: dostawę, zainstalowanie, uruchomienie i przetestowanie zintegrowanego systemu bezpieczeństwa sieci UTM.

§ 3
ZOBOWIĄZANIA WYKONAWCY

1. Wykonawca dostarczy przedmiot umowy na swój koszt i ryzyko do siedziby Zamawiającego.
2. Wykonawca zobowiązuje się do:
   1) dostawy, zainstalowania, uruchomienia i przetestowania fabrycznie nowego i nieużywanego zintegrowanego systemu bezpieczeństwa sieci UTM,
   2) dostawy licencji aktywacyjnych dla funkcji bezpieczeństwa na okres 36 miesięcy,

3) wykonania infrastruktury informatycznej zawierającej:
   a) przygotowanie projektu infrastruktury informatycznej oraz planu wdrożenia zgodnie z wytycznymi Zamawiającego,
   b) zainstalowanie, uruchomienie oraz implementacja planu wdrożenia infrastruktury informatycznej,
   c) przeprowadzenie testów działania oraz testów wysokiej dostępności rozwiązania,
   d) wykonanie dokumentacji powykonawczej,
4) przeprowadzenia jednodniowego szkolenia stanowiskowego dla 2 administratorów w terminie wskazanym przez Zamawiającego.
5) udzielenia wsparcia technicznego przez okres 36 miesięcy liczone od daty odbioru zintegrowanego systemu bezpieczeństwa sieci UTM, zwanego dalej "Systemem", w ramach którego Wykonawca zapewni:
   a) aktualizacje dostarczonego Systemu do nowych wersji oprogramowania, patche, szkolenia administratorów on-site z nowych funkcjonalności,
   b) usługi konsultacyjne w zakresie funkcjonalności, eksploatacji i administrowania Systemem,
   c) bieżące aktualizacje dokumentacji technicznej dla Systemu,
   d) obsługę zgłoszeń problemów dotyczących Systemu poprzez telefon lub e-mail 24 h na dobę 7 dni w tygodniu,

3. Wykonawca w ramach wynagrodzenia umownego zobowiązuje się do udzielenia wsparcia technicznego przez okres 36 miesięcy dla posiadanego przez Zamawiającego systemu logowania i raportowania FortiAnalyzer 1000C w ramach którego Wykonawca zapewni:
   1) aktualizacje posiadanego systemu logowania i raportowania do nowych wersji oprogramowania, patche, szkolenia administratorów on-site z nowych funkcjonalności,
   2) usługi konsultacyjne w zakresie funkcjonalności, eksploatacji i administrowania Systemem FortiAnalyzer 1000C,
   3) bieżące aktualizacje dokumentacji technicznej dla posiadanego systemu,
   4) obsługę zgłoszeń problemów dotyczących posiadanego systemu poprzez telefon lub e-mail 24 h na dobę 7 dni w tygodniu,
4. Wykonawca dostarczy Zamawiającemu przedmiot umowy fabrycznie nowy, nieużywany kompletny, o wysokim standardzie, zarówno pod względem jakości jak i funkcjonalności oraz wolny od wad materiałowych i konstrukcyjnych.
5. W przypadku stwierdzenia podczas odbioru, że dostarczony przedmiot umowy nie odpowiada żądanym przez Zamawiającego minimalnym parametrom technicznym określonym w załączniku nr 9, Wykonawca zobowiązuje się do dokonania wymiany zgodnie z parametrami wskazanymi przez Zamawiającego.
6. Wykonawca oświadcza, że dołączył do oferty oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż posiada autoryzacje producenta w zakresie sprzedaży oferowanego Systemu oraz świadczenia usług z nimi związanych.
7. Wykonawca oświadcza, że dysponuje wiedzą, doświadczeniem oraz uprawnieniami niezbędnymi do należytego wykonania niniejszej umowy oraz zobowiązuje się wykonać przedmiot umowy z należytą starannością z uwzględnieniem obowiązujących przepisów prawa, aktualnej najlepszej wiedzy fachowej a także zasad etyki zawodowej.
8. Wykonawca oświadcza, że podczas realizacji umowy będzie uwzględniał wskazówki Zamawiającego dotyczące sposobu jej wykonywania.

§ 4
ZOBOWIĄZANIA ZAMAWIAJĄCEGO

1. Zamawiający zobowiązuje się do nie rozpakowania przedmiotu umowy przed przybyciem przedstawiciela Wykonawcy.
2. Zamawiający w obecności Wykonawcy dokona odbioru przedmiotu umowy.

3. Zamawiający zobowiązuje się zapłacić Wykonawcy za dostarczony przedmiot umowy zgodnie z ofertą przetargową.

§ 5
WYNAGRODZENIE WYKONAWCY

1. Za wykonanie przedmiotu umowy Wykonawca otrzyma wynagrodzenie w wysokości:

zł netto
(słownie: .....)
zł brutto
(słownie: .....)

2. Podatek VAT został doliczony do ceny netto zgodnie z obowiązującymi przepisami o podatkach.
3. Podstawą wystawienia faktury będzie końcowy protokół odbioru, obejmujący: dostawę, zainstalowanie, uruchomienie i przetestowanie zintegrowanego systemu bezpieczeństwa sieci UTM. oraz protokół z przeprowadzonego instruktażu podpisany przez Zamawiającego i Wykonawcę.
4. Końcowy protokół odbioru podpisany zostanie przez strony w terminie 7 dni roboczych liczonych od dnia zgłoszenia przez Wykonawcę gotowości do odbioru.
5. Zapłata nastąpi przelewem bankowym w terminie 30 dni od dnia otrzymania prawidłowo wystawionej faktury przez Zamawiającego, na konto Wykonawcy wskazane na fakturze.
6. Za termin zapłaty uważa się datę obciążenia rachunku bankowego Zamawiającego.

§ 6
WARUNKI GWARANCJI I NAPRAWY

1. Wykonawca oświadcza, iż udziela 36 - miesięcznej gwarancji producenta:
   1) na przedmiot umowy liczoną od daty jego odbioru.
   2) dla posiadanych przez Zamawiającego urządzeń FortiAP liczoną od daty podpisania umowy.
2. Wykonawca w okresie gwarancji w ramach wynagrodzenia umownego zobowiązuje się do:
   1) przeprowadzenia przeglądów serwisowych nowego systemu bezpieczeństwa sieci UTM, posiadanego systemu centralnego logowania i raportowania FortiAnalyzer 1000C wraz z urządzeniami FortiAP zgodnie ze wskazaniami producenta, nie rzadziej niż raz na 12 miesięcy, (tzn. minimum trzy przeglądy w okresie trwania gwarancji) przy czym ostatni serwis powinien zostać przeprowadzony najpóźniej 3 miesiące po dacie wygaśnięcia okresu gwarancyjnego,
   2) wymiany elementów zużywalnych, których wymiana wchodzi w zakres okresowej obsługi serwisowej przedmiotu umowy,
   3) reakcji serwisu technicznego w ciągu 1 godziny w dni robocze od momentu zgłoszenia awarii Wykonawcy. *„Reakcję serwisu"* rozumie się jako działanie, które ma doprowadzić do usunięcia usterki lub diagnozy uszkodzenia w drodze telefonicznego wywiadu technicznego, serwisu zdalnego lub wizyty osobistej pracownika działu serwisu Wykonawcy,
   4) zakończenia naprawy przedmiotu umowy w terminie do 7 dni roboczych od daty zgłoszenia awarii,
   5) Zamawiający wymaga dostarczenia na czas naprawy, urządzenia zastępczego o parametrach technicznych takich samych lub wyższych w terminie 12 godzin od daty zgłoszenia awarii urządzenia.
   6) wymiany przedmiotu umowy na nowy w przypadku 5 awarii powodujących wyłączenie urządzenia z eksploatacji, w okresie jednego roku trwania gwarancji,
3. W przypadku konieczności wymiany przedmiotu umowy w okresie gwarancji, gwarancja jest wznawiana.

4. Wykonawca zapewni dostępność części zamiennych przez 36 miesięcy od daty podpisania protokołu odbioru.
5. Zamawiający zobowiązuje się do zgłaszania awarii przedmiotu umowy telefonicznie i potwierdzenia zgłoszenia faksem na adres serwisu gwarancyjnego Wykonawcy w .....tel. .....fax. .....
6. Wykonawca zobowiązuje się do potwierdzenia przyjęcia zgłoszenia awarii przez Zamawiającego faxem na nr ..... lub na adres e - mail podany na zgłoszeniu.
7. Wsparcie techniczne w ramach niniejszej umowy będzie realizowane przez podmiot upoważniony przez wytwórcę lub autoryzowanego przedstawiciela do wykonywania tych czynności przez uprawnione osoby wymienione poniżej:
   1) .....
   2) .....

§ 7
OSOBY UPRAWNIONE DO KONTAKTU

Strony wyznaczają niżej wymienione osoby do wzajemnego kontaktowania się przy realizacji przedmiotu umowy:
1) ze strony Zamawiającego – ..... tel..... e-mail:.....
2) ze strony Wykonawcy – ..... tel.: ..... e-mail:.....

§ 8
KARY UMOWNE

1. Wykonawca zobowiązuje się zapłacić Zamawiającemu następujące kary umowne:
   1) w przypadku odstąpienia od umowy przez Zamawiającego z winy Wykonawcy w wysokości 10 % wartości umowy brutto,
   2) za zwłokę w wykonaniu przedmiotu umowy w wysokości 0,2 % wartości umowy brutto, za każdy dzień zwłoki,
   3) za zwłokę w naprawie przedmiotu umowy w wysokości 0,2% wartości umownej brutto za każdy dzień zwłoki
2. Zamawiający zobowiązuje się zapłacić Wykonawcy karę umowną w przypadku odstąpienia od umowy przez Wykonawcę z winy Zamawiającego w wysokości 10% wartości umowy brutto.
3. Zamawiający może dochodzić odszkodowania przewyższającego wysokość zastrzeżonych kar umownych.

§ 9
PODWYKONAWCY

Wykonawca wykona przedmiot umowy we własnym zakresie*) lub przy pomocy podwykonawców*):

1) .....w zakresie .....
2) *)Do zawarcia przez Wykonawcę umowy z podwykonawcą jest wymagana zgoda Zamawiającego. Jeżeli Zamawiający, w terminie 14 dni od przedstawienia mu przez Wykonawcę umowy z podwykonawcą lub jej projektu, nie zgłosi na piśmie sprzeciwu lub zastrzeżeń, uważa się, że wyraził zgodę na zawarcie umowy.

**) niepotrzebne skreślić*

§ 10
ODSTĄPIENIE OD UMOWY

1. Zamawiający może odstąpić od umowy w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy.
2. W przypadkach, o których mowa w ust.1 Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonanej części umowy.

§ 11
ZMIANY UMOWY

Na podstawie art. 144 uPzp, Zamawiający przewiduje możliwość dokonania zmian postanowień zawartej umowy w stosunku do treści oferty na podstawie, której dokonano wyboru Wykonawcy oraz określa warunki tych zmian przez wprowadzenie do zawartej umowy w szczególności aneks dotyczący zmiany terminu realizacji przedmiotu zamówienia w przypadku wystąpienia zmian organizacyjnych leżących po stronie Zamawiającego.

§ 12
POSTANOWIENIA KONCOWE

1. Do spraw nieuregulowanych niniejszą umową mają zastosowanie przepisy ustawy Prawo zamówień publicznych oraz Kodeksu Cywilnego.
2. Wszelkie zmiany do umowy wymagającą formy pisemnej pod rygorem nieważności.
3. Spory wynikłe w związku z niniejszą umową rozstrzygał będzie sąd powszechny właściwy dla siedziby Zamawiającego.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

ZAMAWIAJĄCY **WYKONAWCA**

Załącznik nr 3 do SIWZ
Nr sprawy Szp/FZ – 44/2014

OŚWIADCZENIE WYKONAWCY z art. 22 ust. 1 uPzp

(Wypełnia Wykonawca lub Pełnomocnik w przypadku Konsorcjum albo upoważniona osoba przez Wykonawcę)

1. Dotyczy zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego pn.:

„Dostawa zintegrowanego systemu bezpieczeństwa sieci UTM"

2. Nazwa i adres Wykonawcy *(Pełnomocnika w przypadku Konsorcjum):*

.....

.....

Nazwa i adres Partnera/-ów: *(w przypadku Konsorcjum)*

.....

.....

Niniejszym, zgodnie z art. 22 ust. 1 ustawy z dnia 29.01.2004 r. – Prawo zamówień publicznych oświadczam, że spełniam warunki określone w Specyfikacji Istotnych Warunków Zamówienia, dotyczące:

1. posiadam uprawnienia do wykonywania określonej zamówieniem działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania;
2. posiadam niezbędną wiedzę i doświadczenie;
3. dysponuję odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia;
4. znajduję się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia

Prawdziwość powyższych danych potwierdzam własnoręcznym podpisem, świadom odpowiedzialności karnej z art. 297 k.k.

....., dnia .....

.....
(podpis i pieczątka imienna osoby uprawnionej do reprezentowania Wykonawcy)

Załącznik nr 4 do SIWZ
Nr sprawy Szp/FZ – 44/2014

OŚWIADCZENIE WYKONAWCY o braku podstaw do wykluczenia z art. 24 uPzp

Dotyczy zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego pn.:

„Dostawa zintegrowanego systemu bezpieczeństwa sieci UTM"

Pełna nazwa i adres Wykonawcy:

.....
.....
.....

Niniejszym oświadczam, że:

- nie podlegam wykluczeniu z postępowania o udzielenie zamówienia na podstawie art. 24 ustawy z dnia 29.01.2004 r. – Prawo zamówień publicznych.

Prawdziwość powyższych danych potwierdzam własnoręcznym podpisem, świadom odpowiedzialności karnej z art. 297 k.k.

....., dnia .....

.....
(podpis i pieczątka imienna osoby uprawnionej do reprezentowania Wykonawcy)

Załącznik nr 5 do SIWZ
Nr sprawy Szp/FZ – 44/2014

INFORMACJA O PRZYNALEZNOŚCI DO TEJ SAMEJ GRUPY KAPITAŁOWEJ

Dotyczy zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego pn.:

„Dostawa zintegrowanego systemu bezpieczeństwa sieci UTM"

Informuję, że **należę* / nie należę*** 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.).*

**) wybrać odpowiednio*

W przypadku zaznaczenia słowa „należę" konieczne jest dołączenie wykazu podmiotów wchodzących w skład tej samej grupy kapitałowej.

Prawdziwość powyższych danych potwierdzam własnoręcznym podpisem, świadom odpowiedzialności karnej z art. 297 k.k.

....., dnia .....

.....
(podpis i pieczątka imienna osoby uprawnionej do reprezentowania Wykonawcy)

Załącznik nr 6 do SIWZ
Nr sprawy Szp/FZ – 44/2014

WYKAZ OSÓB I PODMIOTÓW, KTÓRE UCZESTNICZYĆ BĘDĄ W WYKONANIU ZAMÓWIENIA

1. Dotyczy zamówienia publicznego Nr ***Szp/FZ – 44/2014*** pod nazwą:

„Dostawa zintegrowanego systemu bezpieczeństwa sieci UTM"

Wykaz osób, które będą uczestniczyć w wykonaniu zamówienia w szczególności odpowiedzialnych za świadczenie usług wraz z informacjami na temat ich kwalifikacji zawodowych, doświadczenia i wykształcenia niezbędnych do wykonywania zamówienia, także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami

Lp.	Imię i nazwisko	Stanowisko i zakres obowiązków	Kwalifikacje zawodowe*)	Doświadczenie zawodowe (staż i przebieg pracy)	Wykształcenie	Podstawa dysponowania
1						
2						
3						
4						

**)należy podać nazwę i numer certyfikatu*

....., dnia .....

.....
(podpis i pieczątka imienna osoby uprawnionej do reprezentowania Wykonawcy)

Załącznik nr 7 do SIWZ
Nr sprawy Szp/FZ – 44/2014

WYKAZ GŁÓWNYCH DOSTAW

Dotyczy zamówienia publicznego Nr Szp/FZ – 44/2014 pod nazwą:

„Dostawa zintegrowanego systemu bezpieczeństwa sieci UTM"

Nazwa podmiotu i miejsce wykonania dostaw	*Rodzaj zamówienia wraz zakresem rzeczowym*	*Czas realizacji (należy podać daty)*		*Wartość*
		początek	*koniec*	

Uwaga ! należy załączyć dowody potwierdzające należyte wykonanie dostawy

....., dnia .....

.....
(podpis i pieczątka imienna osoby
uprawnionej do reprezentowania Wykonawcy)

Załącznik nr 8 do SIWZ
Nr sprawy: Szp/FZ – 44/2014

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

§ 1.

Dostarczony zintegrowany system bezpieczeństwa sieci UTM musi składać się z co najmniej dwóch urządzeń pracujących w klastrze. Dostarczone urządzenia powinny zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. Każde z urządzeń powinno charakteryzować się następującymi parametrami:

1. Możliwość łączenia dostarczonych urządzeń w klaster Active-Active lub Active-Passive. W ramach postępowania dostawca powinien dostarczyć system w formie redundantnej w postaci klastra urządzeń.
2. Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo, przy użyciu układu ASIC. Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta. Producent udzieli odbiorcy licencji na nielimitowaną ilość chronionych użytkowników.
3. Elementy systemu realizujące funkcję Firewall oraz VPN powinny być wyposażone w redundantne zasilacze.
4. Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia.
5. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
6. Monitoring stanu realizowanych połączeń VPN.
7. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.
8. System realizujący funkcje Firewall powinien dysponować minimum 2 portami Ethernet 10 Gbps Ethernet oraz 12 portami 1 Gbps TX oraz 8 gniazdami typu SFP.
9. System powinien posiadać co najmniej dwie pary portów bypass.
10. Możliwość tworzenia min 254 interfejsów wirtualnych definiowanych jako VLANy W oparciu o standard 802.1Q.
11. W zakresie Firewall'a obsługa nie mniej niż 7 milionów jednoczesnych połączeń oraz 190 tys. Nowych połączeń na sekundę
12. Przepustowość Firewall'a: nie mniej niż 20 Gbps
13. Wydajność szyfrowania VPN IPSec: nie mniej niż 8 Gbps
14. System realizujący funkcję Firewall powinien być wyposażony W lokalny dysk o pojemności minimum 120GB do celów logowania i raportowania oraz realizowania funkcjonalności optymalizacji dostępu do zasobów pobieranych z sieci Internet.
15. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane W postaci osobnych platform sprzętowych lub programowych:
    1) kontrola dostępu - zapora ogniowa klasy Stateful Inspection
    2) ochrona przed wirusami antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS).
    3) poufność danych - połączenia szyfrowane IPSec VPN oraz SSL VPN
    4) ochrona przed atakami - Intrusion Prevention System [IPS] możliwość zdefiniowania co najmniej 80 sensorów ochrony przed atakami.

5) kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
6) kontrola zawartości poczty - antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
7) kontrola pasma oraz ruchu (QoS, Traffic shaping)
8) Kontrola aplikacji oraz rozpoznawanie ruchu P2P
9) Możliwość analizy ruchu szyfrowanego protokołem SSL
10) Ochrona przed wyciekiem poufnej informacji (DLP) z funkcją archiwizowania informacji. Możliwość zdefiniowania min 80 różnych sensorów wykrywania wycieków danych.

16. Wydajność skanowania ruchu W celu ochrony przed atakami (IPS) min 6 Gbps
17. Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączoną funkcją: Antivirus min. 1.7 Gbps skanowanie w trybie proxy.
18. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
    1) Tworzenie połączeń W topologii Site-to-Site oraz Client-to-Site
    2) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
    3) Praca w topologii Hub and Spoke oraz Mesh
    4) Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF
    5) Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
19. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPV2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować również w ramach terminowanych na urządzeniu połączeniach IPSec VPN
20. Możliwość budowy min 10 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a z możliwością rozbudowy do co najmniej 20. Jeśli rozbudowa powyżej 10 wirtualnych urządzeń wymaga dodatkowej licencji zamawiający nie wymaga jej dostarczenia a jedynie zapewnienia możliwości jej zastosowania w późniejszym terminie.
21. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
22. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)
23. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
24. Silnik antywirusowy powinien umożliwiać skanowanie ruchu W obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
25. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 5000 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.
26. Funkcja kontroli aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
27. Baza filtra WWW o wielkości co najmniej 45 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 oraz tworzenia wyjątków i reguł omijania filtra WWW.
28. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
29. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
    1) haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu,
    2) haseł statycznych i definicji użytkowników przechowywanych W bazach zgodnych z LDAP,
    3) haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych,

4) rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny.

30. Zamawiający wymaga dostarczenia 5 tokenów sprzętowych zabezpieczających dostęp administracyjny do urządzenia oraz połączeń VPN poprzez rozszerzenie autentykacji o dodatkowy kod generowany z tokena.
31. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:
    1) ICSA dla funkcjonalności SSLVPN, IPS, Antywirus
    2) ICSA lub EAL4 dla funkcjonalności Firewall
32. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

§ 2

1. Każde z dostarczonych urządzeń wchodzących w skład systemu bezpieczeństwa sieci UTM nie może przekraczać rozmiaru 2U w szafie rack.
2. Każde z dostarczonych urządzeń powinno posiadać dwa wewnętrzne redundantne zasilacze wymieniane w tracie pracy urządzenia.

§ 3

1. Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres 36 miesięcy.

Dotyczy zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego pn.:

„Dostawa zintegrowanego systemu bezpieczeństwa sieci UTM"

Zintegrowany system bezpieczeństwa sieci UTM musi spełniać następujące parametry:

Lp.	Parametr	Opis wymaganych parametrów technicznych i cech oferowanego systemu celem wykazania zgodności z opisem przedmiotu zamówienia	Opis parametrów oferowanych
1	*2*	*3*	*4*
1.	Architektura systemu	Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo, przy użyciu układu typu ASIC lub równoważnego układu specyfikowanego. **Jednocześnie**, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta. Producent udzieli odbiorcy licencji na nielimitowaną ilość chronionych użytkowników (licencja na urządzenie). Proponowane urządzenia muszą zostać dostarczone w formie klastra HA w celu zapobiegania potencjalnym przestojom w razie awarii.	
2.	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. **Uwaga**: Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia.	
3.	Ilość/rodzaj portów	Nie mniej niż: **12 portów Ethernet 10/100/1000Tx, 8 portów SFP oraz minimum 2 porty 10 Gbps SFP+** dostępnych na każdym dostarczonym urządzeniu.	
4.	Funkcjonalności podstawowe i uzupełniające	System ochrony musi obsługiwać wszystkie z poniższych funkcjonalności podstawowych: 1. **kontrolę dostępu** - zaporę ogniową klasy [**FW**] Stateful Inspection 2. **ochronę przed wirusami** – antywirus [**AV**] (SMTP, POP3, IMAP, http, FTP, IM) min. 15000 sygnatur indywidualnych wirusów 3. **poufność danych** - IPSec **VPN** oraz SSL VPN 4. **ochronę przed atakami** - Intrusion Prevention System [**IPS** i **IDS**] 5. **kontrolę pasma** [**QoS**] oraz **ruchu** i [Traffic Shaping] 6. **kontrolę treści** – Web Filter [**WF**] dla min. 45 mln URL 7. **kontrolę zawartości poczty** – antyspam [**AS**] dla protokołów SMTP, POP3, IMAP 8. **kontrolę aplikacji** np aplikacji P2P, Gadugadu itp. dla min 4500 aplikacji 9. **optymalizacja WAN** 10. **kontrolę danych wychodzących z sieci** – sensory DLP co najmniej 80 sensorów. 11. **możliwość tworzenia wirtualnych systemów bezpieczeństwa** – w celu zapewnienia możliwości segmentacji sieci. 12. **kontrola ruchu SSL** – skanowanie antywirusowe ruchu SSL oraz funkcjonalności uzupełniających: **13. IDS** – możliwość użycia niewykorzystanych portów jako system wykrywania włamań. **14. Kontrola dostępu do sieci** - NAC	
5.	Zasada działania (tryby)	Urządzenie powinno dawać możliwość ustawienia jednego z dwóch trybów pracy: • router / NAT • most /transparent bridge/ Tryb przezroczysty umożliwia wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu.	

6.	Polityka bezpieczeństwa (firewall)	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników aplikacji, domeny, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (m.in. pasma gwarantowane i maksymalne, priorytety, oznaczenia DiffServ). **Uwaga:** system musi umożliwiać zaimplementowanie jednocześnie **minimum 90 000 polityk bezpieczeństwa** dla urządzeń zabezpieczających.	
7.	Wykrywanie ataków	Wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów (m.in. Java/ActiveX), oraz exploitów. Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP. 1) Nie mniej niż 5000 sygnatur ataków. 2) Aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie 3) Możliwość wykrywania anomalii protokołów i ruchu	
8.	Translacja adresów	Statyczna i dynamiczna translacja adresów (NAT). Translacja NAPT.	
9.	Wirtualizacja i routing dynamiczny	Możliwość definiowania w jednym urządzeniu wirtualnych routerów, gdzie każdy z nich posiada indywidualne tabele routingu. Urządzenie może wykonywać routing IP na bazie adresu przeznaczenia pakietów oraz adresu źródłowego. Możliwość budowy min 10 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a z możliwością rozbudowy do co najmniej 20. Jeśli rozbudowa powyżej 10 wirtualnych urządzeń wymaga dodatkowej licencji zamawiający nie wymaga jej dostarczenia a jedynie zapewnienia możliwości jej zastosowania w późniejszym terminie. Obsługa Policy Routingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego. Protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM.	
10.	Optymalizacja	System musi wspierać **optymalizację WAN**, przyspieszenie działania aplikacji w sieci WAN, korzystając z nowoczesnych technik optymalizacji takich jak: optymalizacja protokołów, byte caching, web caching.	
11.	Połączenia VPN	Wymagane nie mniej niż: Tworzenie połączeń w topologii VPN: Meshed Site-to-site lub Hub-Spoke Site-to-site Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności Konfiguracja w oparciu o politykę bezpieczeństwa (Policy-based VPN) Obsługa IPSec NAT Traversal dla konfiguracji VPN Client-to-site oraz Site-to-site *Interface base VPN* umożliwiający rozgłaszanie tunelu przez dynamiczne protokoły routingu.	
12.	Uwierzytelnianie użytkowników	System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia, zgodnych z LDAP, w bazie ActiveDirectory oraz haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych.	
13.	PKI	Urządzenie musi współpracować z wiodącymi urzędami certyfikacji, nie mniej niż: Verisign, Entrust, Microsoft	
14.	Wydajność	System musi zapewnić obsługę minimum **4 000** użytkowników sieci: • Przepływność firewalla nie mniejsza niż: **20 Gb/s; (przy pakietach UDP 1500 bajtów jak 64 bajtów)** • Przepływność dla VPN/IPSec nie mniejsza niż: **8Gb/s** • Przepływność dla skanowania antywirusowego nie mniejsza niż: **1,7 Gbps dla trybu PROXY.** • Przepływność dla IPS nie mniejsza niż: **6 Gb/s** • Ilość jednoczesnych sesji nie mniejsza niż: **7 000 000**	

15.	Funkcjonalność i niezawodność	System musi wspierać monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych urządzeń zabezpieczeń i dostępu oraz łączy sieciowych. Możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive	
16.	Konfiguracja i zarządzanie	Możliwość konfiguracji poprzez terminal i linię komend oraz konsolę graficzną (GUI). Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji. Musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. Administratorzy muszą być uwierzytelniani za pomocą: haseł statycznych, haseł dynamicznych (RADIUS, RSA SecureID). System powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB.	
17.	Lokalne miejsce przechowywania	System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 120GB do celów logowania i raportowania oraz realizowania funkcjonalności optymalizacji dostępu do zasobów pobieranych z sieci Internet.	
18.	Logowanie i Raportowanie	Administrator musi mieć możliwość zbierania logów z urządzenia [grupy urządzeń], tworzenia raportów przez dedykowaną, sprzętową platformę raportującą,. Centralny system zbierania logów powinien umożliwiać: • Tworzenie dziennika zdarzeń z logów urządzeń ochronnych • Generowanie raportów aktywności sieci oraz zdarzeń bezpieczeństwa. • Kwarantannę podejrzanych plików [z modułu antywirusowego] • Urządzenie musi mieć możliwość integracji z posiadanym systemem logowania i raportowania FortiAnalyzer 1000C.	
19.	Integracja	Dostarczone rozwiązanie musi być kompatybilne z posiadanym przez Zamawiającego urządzeniami FortiAP na poziomie zarządzania politykami firewall i reguł bezpieczeństwa.	
20.	Budowa	Wszystkie elementy systemu muszą pozwalać na montaż w szafie RACK 19". Maksymalna wysokość każdego dostarczonego urządzenia 2RU w szafie rack.	
21.	Zasilanie	Parametry zasilania 220V. Urządzenie powinno być wyposażone w dwa wewnętrzne zasilacze wymienialne w trakcie przy urządzenia.	
22.	Gwarancja producenta	Gwarancja producenta 36 miesięcy, o parametrach zgodnych z opisem zawartym w SIWZ.	
23.	Wsparcie dostawcy	Wsparcie techniczne wykonawcy na 36 miesięcy, o parametrach zgodnych z opisem zawartym w SIWZ.	
24.	Wyposażenie dodatkowe	5 tokenów sprzętowych zabezpieczających dostęp administracyjny do urządzenia oraz połączeń VPN poprzez rozszerzenie autentykacji o dodatkowy kod generowany z tokena.	
25.	Wymagane certyfikaty	a. ICSA dla funkcjonalności SSLVPN, IPS, Antywirus b. ICSA lub EAL4 dla funkcjonalności Firewall	

) w kolumnie należy opisać parametry oferowane i podać zakresy

Parametry określone w kolumnie nr 3 są parametrami granicznymi, których nie spełnienie spowoduje odrzucenie oferty. Brak opisu w kolumnie 4 będzie traktowany jako brak danego parametru w oferowanej konfiguracji urządzeń.

.....

(podpis i pieczątka imienna osoby uprawnionej do reprezentowania Wykonawcy)