SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

1. Nazwa (firma) oraz adres zamawiającego

Lubelski Oddział Wojewódzki Narodowego Funduszu Zdrowia
ul. Szkolna 16, 20-124 Lublin, tel. (0-81) 53-105-11, fax (0-81) 53-105-28

2. Tryb udzielenia zamówienia

Postępowanie o udzielenie zamówienia prowadzone jest na zasadach określonych w ustawie z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j DzU. z 2013 r. poz. 907) w trybie przetargu nieograniczonego o wartości zamówienia nie przekraczającej kwot określonych w przepisach wydanych na podstawie art. 11 ust. 8 ww. ustawy.

3. Opis przedmiotu zamówienia

Modernizacja infrastruktury sieci WAN

Szczegółowy opis przedmiotu zamówienia zawarty jest w **załączniku nr 7** do specyfikacji.

4. Termin wykonania zamówienia

Termin realizacji zmówienia: do 30 dni od podpisania umowy.

5. **Warunki udziału w postępowaniu oraz opis sposobu dokonywania oceny spełniania tych warunków**

O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy spełniają warunki, o których mowa w art. 22 ust. 1 ustawy Prawa zamówień publicznych, dotyczące:

5.1.1. posiadania uprawnień do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania;

Zamawiający nie precyzuje w tym zakresie wymagań. Ocena spełnienia w/w warunku udziału w postępowaniu nastąpi na podstawie oświadczenia załączonego do oferty.

5.1.2. posiadania wiedzy i doświadczenia

warunkiem udziału w postępowaniu jest wykonanie (w przypadku świadczeń okresowych lub ciągłych uwzględniane będą również zamówienia wykonywane) w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy w tym okresie co najmniej 2 (dwóch) zamówień polegających na dostawie urządzeń sieciowych wartości nie mniejszej niż 100 000 złotych brutto.

Ocena spełnienia tego warunku nastąpi na podstawie wykazu wykonanych (a w przypadku świadczeń okresowych lub ciągłych również wykonywanych) zamówień, z dokumentami potwierdzającymi, że zamówienia te zostały wykonane lub są wykonywane należycie, zgodnie **z załącznikiem nr 4** do specyfikacji.

5.1.3. dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia,

Zamawiający wymaga aby Wykonawca dysponował co najmniej dwoma certyfikowanymi inżynierami autoryzowanymi przez producenta dostarczanych urządzeń. Ocena spełnienia w/w warunku udziału w postępowaniu nastąpi na podstawie oświadczenia załączonego do oferty.

5.1.4. sytuacji ekonomicznej i finansowej.

Zamawiający nie precyzuje w tym zakresie wymagań. Ocena spełnienia w/w warunku udziału w postępowaniu nastąpi na podstawie oświadczenia załączonego do oferty.

oraz nie podlegają wykluczeniu z postępowania o udzielenie zamówienia publicznego na podstawie art. 24 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych.

5.2. Zamawiający oceni spełnienie warunków udziału w postępowaniu na podstawie dokumentów i oświadczeń załączonych do oferty metodą spełnia-nie spełnia.

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

oddania mu do dyspozycji niezbędnych zasobów na okres korzystania z nich przy wykonaniu zamówienia.

5.4. W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia warunek udziału w postępowaniu, o którym mowa **w pkt 5.1.2** musi zostać spełniony przez wykonawców łącznie zaś brak podstaw do wykluczenia z postępowania o udzielenie zamówienia wykonawcy, w okolicznościach o których mowa w art. 24 ustawy prawo zamówień publicznych, musi zostać wykazany przez każdego z wykonawców.

5.5. Oferty wykonawców, którzy wykażą spełnianie wymaganych warunków zostaną dopuszczone do badania i oceny. Wykonawcy, którzy nie wykażą spełniania wymaganych warunków zostaną wykluczeni z postępowania.

W celu potwierdzenia spełnienia opisanych wyżej warunków Oferent musi załączyć do oferty dokumenty określone w rozdziale 6.

6. Wykaz oświadczeń i dokumentów, jakie mają dostarczyć wykonawcy w celu potwierdzenia spełniania warunków udziału w postępowaniu oraz nie podlegania wykluczeniu na podstawie art. 24 ustawy.

6.1. Wykaz oświadczeń i dokumentów:

6.1.1. Aktualny odpis z właściwego rejestru lub centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust. 1 pkt 2 ustawy prawo zamówień publicznych, wystawionego nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert, a w stosunku do osób fizycznych oświadczenie w zakresie art. 24 ust. 1 pkt 2 ustawy, według załącznika nr 3 do specyfikacji.

6.1.2. Oświadczenie Wykonawcy, że spełnia warunki określone w art. 22 ust. 1 ustawy prawo zamówień publicznych według **załącznika nr 2** do specyfikacji.

6.1.3. Oświadczenie Wykonawcy, że nie podlega wykluczeniu z postępowania na podstawie art. 24 ustawy prawo zamówień publicznych według **załącznika nr 3** do specyfikacji.

6.1.4. Wykaz wykonanych głównych dostaw, w zakresie niezbędnym do wykazania spełniania warunku wiedzy i doświadczenia, określonego w **rozdz. 5.1.2** w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów na rzecz których dostawy zostały wykonane, według **załącznika nr 4** do specyfikacji, wraz z załączeniem dowodów czy zostały wykonane należycie.

6.1.5. Listę podmiotów należących do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5 ustawy lub oświadczenie, że Wykonawca nie należy do grupy kapitałowej, zgodnie z **załącznikiem nr 3** do specyfikacji.

6.2. Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentu określonego w **pkt. 6.1.1** przedkłada dokument wystawiony w kraju, w którym ma siedzibę lub miejsce zamieszkania potwierdzający, że nie otwarto jego likwidacji ani nie ogłoszono upadłości - wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia albo składania ofert.

6.3. Jeżeli w miejscu zamieszkania osoby lub w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentu, o którym mowa w **pkt. 6.2**, zastępuje się go dokumentem zawierającym oświadczenie złożone przed notariuszem, właściwym organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego odpowiednio miejsca zamieszkania osoby lub kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania - wystawionym nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

6.4. W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia dokumenty wymagane w **pkt. 6.1.1 – 6.1.3** winien złożyć każdy wykonawca. Warunki udziału w postępowaniu określone **w rozdz. 5.1.2 i 5.1.3** musi spełniać co najmniej jeden Wykonawca lub warunek ten Wykonawcy mogą spełniać łącznie.

6.5. Wykonawcy ubiegający się wspólnie o udzielenie zamówienia muszą ustanowić pełnomocnika do reprezentowania ich w postępowaniu albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Fakt ustanowienia pełnomocnika musi

wynikać z załączonych do oferty dokumentów (np. pełnomocnictwa). Dokument pełnomocnictwa musi być złożony w oryginale lub poświadczonej notarialnie za zgodność z oryginałem kopii.

7. Informacje o sposobie porozumiewania się zamawiającego z wykonawcami oraz przekazywania oświadczeń i dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z wykonawcami.

7.1. W niniejszym postępowaniu wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje zamawiający i wykonawca przekazują pisemnie, faxem lub drogą elektroniczną.

7.2. Osobą upoważnioną do kontaktowania się z wykonawcami jest Jolanta Pietrasińska, tel. 53-105-11, fax 53-105-28, e-mail: jolanta.pietrasinska@nfz-lublin.pl

7.3. Adres strony internetowej, na której zamieszczone jest ogłoszenie o zamówieniu oraz specyfikacja istotnych warunków zamówienia: www.nfz-lublin.pl
Na stronie tej zamawiający będzie zamieszczał również inne informacje wymagane prawem zamówień publicznych związane z niniejszym postępowaniem.

7.4. Zamawiający nie przewiduje zwoływania zebrania wszystkich wykonawców w celu wyjaśnienia wątpliwości dotyczących treści specyfikacji istotnych warunków zamówienia.

8. Wymagania dotyczące wadium

Zamawiający nie wymaga wniesienia wadium.

9. Termin związania ofertą.

Każdy wykonawca będzie związany swoją ofertą 30 dni od upływu terminu składania ofert.

10. Opis sposobu przygotowania ofert.

10.1. Ofertę należy napisać pismem czytelnym w języku polskim. Dokumenty składające się na ofertę sporządzone w języku obcym winny być składane wraz z tłumaczeniem na język polski, poświadczonym przez wykonawcę.

10.2. Dokumenty składające się na ofertę powinny być podpisane przez osobę upoważnioną do występowania w imieniu wykonawcy, uprawnioną zgodnie z odpisem z Krajowego Rejestru Sądowego lub z zaświadczeniem o wpisie do ewidencji działalności gospodarczej albo przez osobę umocowaną przez osobę uprawnioną, a w przypadku składania oferty wspólnej - przez pełnomocnika wykonawców składających ofertę wspólną.
Poprawki powinny być naniesione czytelnie oraz opatrzone podpisem osoby upoważnionej.

10.3. Wykonawcy zobowiązani są złożyć następujące dokumenty oraz oświadczenia:

10.3.1. Formularz oferty zgodnie z **załącznikiem nr 1**,

10.3.2. Oświadczenia i dokumenty wymagane w **rozdziale 6** specyfikacji istotnych warunków zamówienia,

10.3.3. Pełnomocnictwo do reprezentowania w postępowaniu albo do reprezentowania w postępowaniu i zawarcia umowy, w przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia.

10.3.4. wykaz wykonanych zamówień, zgodnie z **załącznikiem nr 4** do specyfikacji wraz dowodami potwierdzającymi, że zamówienia te zostały wykonane lub są wykonywane należycie,

10.3.5. Formularz kosztorysu ofertowego zgodnie **załącznikiem nr 5**.

10.3.6. Warunki usług gwarancyjnych zgodnie z **załącznikiem nr 6**.

10.3.7. Szczegółowy opis przedmiotu oferty – opracowanie własne oferenta, zawierające opis procesu modernizacji.

10.4. Ofertę należy złożyć w trwale zamkniętej kopercie zaadresowanej: Lubelski Oddział Wojewódzki NFZ, ul. Szkolna 16, 20-124 Lublin oraz posiadającej następujące oznaczenie „ Oferta na modernizację infrastruktury sieci WAN ”, nie otwierać przed 10.04.2015 r. godz. 14.15”. Kopertę należy opatrzyć pieczęcią firmową wykonawcy lub nazwą, adresem, numerami telefonu i faksu wykonawcy.

11. Miejsce oraz termin składania i otwarcia ofert.

Oferty winny wpłynąć do siedziby Lubelskiego Oddziału Wojewódzkiego NFZ, ul. Szkolna 16, 20-124, Lublin, pokój nr 20 w terminie do dnia 10.04.2015 r. do godziny 14.00. Decyduje data i godzina wpływu oferty do Zamawiającego, a nie data jej wysłania przesyłką pocztową czy kurierską. Zamawiający niezwłocznie zwraca ofertę, która została złożona po terminie. Otwarcie ofert nastąpi w siedzibie Zamawiającego w Sali Konferencyjnej, pokój nr 205, w dniu 10.04.2015 r. o godzinie 14.15.

12. Opis sposobu obliczenia ceny

12.1. Oferent określi cenę za całość zamówienia zgodnie z formularzem kosztorysu ofertowego stanowiącym **załączniki nr 5**. Cena powinna zawierać w sobie ewentualne upusty proponowane przez oferenta (niedopuszczalne są żadne negocjacje cenowe).

12.2. W cenie oferty Oferent ujmie następujące koszty:

12.2.1. dostarczenie przedmiotu umowy do siedziby Zamawiającego i wniesienia przez pracowników oferenta do pomieszczeń wskazanych przez Zamawiającego,

12.2.2. dokonania instalacji, konfiguracji i uruchomienia,

12.2.3. nieodpłatnego serwisu gwarancyjnego,

12.2.4. przeszkolenia personelu Zamawiającego w zakresie obsługi,

13. Opis kryteriów, którymi zamawiający będzie się kierował przy wyborze oferty wraz z podaniem znaczenia tych kryteriów oraz sposobu oceny ofert.

Przy wyborze oferty zamawiający będzie się kierował następującymi kryteriami oceny ofert.

1. Cena – 95%

Liczba punktów dla kryterium ceny obliczona zostanie wg wzoru:
cena oferty najkorzystniejszej/cena oferty rozpatrywanej x 95.

2. Termin realizacji – 5%

Liczba punktów dla kryterium termin realizacji obliczona zostanie wg wzoru:
najkrótszy oferowany termin realizacji (w dniach)/termin realizacji w ofercie rozpatrywanej x 5

Za najkorzystniejszą zostanie uznana oferta, która uzyska największą sumę punktów obliczonych dla poszczególnych kryteriów zgodnie z ww. wzorami.

14. Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego.

Wykonawca, którego oferta zostanie wybrana zobowiązany jest podpisać umowę zgodnie ze specyfikacją istotnych warunków zamówienia, w miejscu i terminie wskazanym przez zamawiającego.

15. Wymagania dotyczące wadium i zabezpieczenia należytego wykonania umowy.

Zamawiający nie wymaga wnoszenia wadium i zabezpieczenia należytego wykonania umowy.

16. Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia publicznego, ogólne warunki umowy albo wzór umowy, jeżeli zamawiający wymaga od wykonawcy, aby zawarł z nim umowę w sprawie zamówienia publicznego na takich warunkach

Do specyfikacji dołączony jest wzór umowy stanowiący jej integralną część.

17. Pouczenie o środkach ochrony prawnej przysługujących wykonawcy w toku postępowania o udzielenie zamówienia.

Wykonawcom a także innym osobom, jeżeli ich interes prawny w uzyskaniu zamówienia doznał lub może doznać uszczerbku w wyniku naruszenia przez Zamawiającego przepisów ustawy, przysługują środki ochrony prawnej zgodnie z Działem VI ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych.

18. Oferty częściowe

Zamawiający nie dopuszcza składania ofert częściowych.

19. Umowa ramowa

Zamawiający nie przewiduje zawarcia umowy ramowej

20. Informacja o przewidywanych zamówieniach uzupełniających

Zamawiający nie przewiduje udzielania zamówień uzupełniających.

21. Oferty wariantowe

Zamawiający nie dopuszcza możliwości składania ofert wariantowych.

22. Informacja dotycząca walut obcych

Zamawiający nie przewiduje możliwości prowadzenia rozliczeń w walutach obcych.

23. Informacja dotycząca kosztów postępowania

Zamawiający nie przewiduje możliwości zwrotu kosztów udziału w postępowaniu.

24. Podwykonawcy

Zamawiający prosi o wskazanie części zamówienia, którą oferent zamierza powierzyć podwykonawcom.

Podpisy członków komisji przetargowej:

1. Joanna Klimkowska .....
2. Robert Szostakiewicz .....
3. Wojciech Kwit .....
4. Jolanta Pietrasińska .....

ZATWIERDZAM

.....

Załącznik nr 1

OFERTA

z dnia .....

Dane oferenta:
nazwa.....
siedziba.....
nr telefonu ....., nr faxu .....
internet: http:// ..... e-mail .....
REGON.....

Do:
Narodowy Fundusz Zdrowia Lubelski Oddział Wojewódzki
ul. Szkolna 16, **20-124 Lublin**

Oferujemy realizację zamówienia dotyczącego modernizacji infrastruktury sieci WAN, zgodnie ze specyfikacją istotnych warunków zamówienia za kwotę:

brutto ..... zł.

(słownie .....)

w tym kwota netto wynosi ..... zł

(słownie .....)

podatek VAT w wysokości ..... zł

(słownie .....)

1. Szczegółowa charakterystyka przedmiotu oferty stanowi załącznik nr ..... .
2. Zamówienie wykonamy w terminie do ..... .
3. Oświadczamy, że uważamy się za związanych niniejszą ofertą przez 30 dni od terminu składania ofert.
4. Oświadczamy, że zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia umowy w miejscu i terminie wyznaczonym przez zamawiającego.
5. Osobą/osobami upoważnionymi do podpisania umowy są:

   .....
   (imię nazwisko, stanowisko)

6. Oświadczamy, że w rozliczeniach obowiązywać będzie 21 dniowy termin płatności.

7. Wskazanie części zamówienia, którą wykonawca zamierza powierzyć podwykonawcom

.....

Podpisano
(upoważniony przedstawiciel oferenta)

Załącznik nr 2

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

.....
nazwa i adres oferenta

OŚWIADCZENIE WYKONAWCY

w trybie art. 22 ust. 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych
(tekst jednolity Dz. U. z 2010 r. Nr 113, poz. 759 z późn. zm.)

Przystępując do postępowania o udzielenie zamówienia publicznego dotyczącego modernizacji infrastruktury sieci WAN oświadczam, że firma, którą reprezentuję spełnia warunki dotyczące:

1. posiadania uprawnień do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania;
2. posiadania wiedzy i doświadczenia;
   Oświadczam, że dysponuję dwoma certyfikowanymi inżynierami autoryzowanymi przez producenta dostarczanych urządzeń.
3. dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonywania zamówienia;
4. sytuacji ekonomicznej i finansowej.

.....
podpis upoważnionego przedstawiciela oferenta

Załącznik nr 3

OŚWIADCZENIE WYKONAWCY O BRAKU PODSTAW DO WYKLUCZENIA

.....

.....

nazwa (firma) i adres Wykonawcy

1. Oświadczam/y, że nie podlegam/y wykluczeniu z postępowania o udzielenie zamówienia na podstawie art. 24 ustawy z dnia 29 stycznia 2004 r. prawo zamówień publicznych (t.j. Dz. U. z 2010 r. Nr 113, poz. 759 ze zm.) w postępowaniu o udzielenie zamówienia publicznego dotyczącym modernizacji infrastruktury sieci WAN.

2. Oświadczam/y, że nie jestem/eśmy członkiem grupy kapitałowej*

.....
podpis upoważnionego przedstawiciela oferenta

∗ W sytuacji gdy Wykonawca jest członkiem grupy kapitałowej należy skreślić oświadczenie zawarte w pkt. 2 i załączyć listę podmiotów należących do tej samej grupy kapitałowej,
o której mowa w art. 24 ust. 2 pkt 5 ustawy.

Załącznik nr 4

.....
nazwa i adres oferenta

Wykaz wykonanych zamówień

Wykaz wykonanych w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, zamówień polegających na dostawie urządzeń sieciowych o wartości nie mniejszej niż 100 000 złotych brutto.

Przedmiot zamówienia	Wartość zamówienia	czas realizacji (należy podać daty)		nazwa i adres Zamawiającego
		początek	Koniec	

W załączeniu dowody potwierdzające należyte wykonanie ww. zamówień ..... sztuk.

Podpisano
(upoważniony przedstawiciel oferenta)

Załącznik nr 5

.....
nazwa i adres oferenta

Formularz kosztorysu ofertowego

Nazwa	Ilość	Gwarancja *	Wartość całkowita brutto
Modernizacja infrastruktury sieci WAN	1		

*w kolumnie gwarancja proszę podać długość gwarancji w miesiącach oraz czyja to jest gwarancja – producenta lub dostawcy.

Razem wartość całkowita brutto słownie:

.....

Podpisano
(upoważniony przedstawiciel oferenta)

Załącznik nr 6

.....
nazwa i adres oferenta

Warunki usług gwarancyjnych i wsparcia serwisowego

I. Warunki usług gwarancyjnych

1. Okres gwarancji (maintenance producenta w zakresie sprzętu i oprogramowania) w miesiącach liczony od daty ostatecznego, bezusterkowego odbioru przedmiotu zamówienia zgodnie

z formularzem kosztorysu ofertowego wynosi …… miesięcy *(minimum 12)*.

2. Usługi serwisowe będą wykonywane przez Podmiot, posiadający autoryzację Producenta bądź jego przedstawiciela w Polsce, do ich świadczenia na terenie kraju.

   Adres, telefon i fax punktu serwisowego : .....

   …….

3. Czas reakcji serwisu od momentu powiadomienia - **4 godziny**.

4. Zgłoszenie naprawy serwisowej następuje faxem lub e-mailem przy czym dopuszcza się powiadomienie telefonicznie z późniejszym potwierdzeniem faxem lub e-mailem.

5. Wykonawca musi okazać zaświadczenie informujące o możliwości przyjęcia uszkodzonego urządzenia objętego gwarancją do naprawy w autoryzowanym serwisie na terenie całego kraju.

6. W przypadku ujawnienia się w okresie gwarancji wad fizycznych Sprzętu lub zużycia świadczącego o niższej jakości niż zapewniana, Gwarant zobowiązuje się do nieodpłatnego usunięcia tych wad poprzez naprawę sprzętu lub wymianę elementów, które uległy pogorszeniu.

7. Wszelkie koszty transportu rzeczy wadliwej oraz zastępczej obciążają Gwaranta.

8. Po trzeciej awarii Wykonawca wymieni sprzęt na nowy.

9. Ze strony Dostawcy osobą odpowiedzialną za koordynację jest .....

Podpisano
(upoważniony przedstawiciel oferenta)

II . Warunki wsparcia serwisowego

Dla wszystkich zamawianych elementów oferujemy wsparcie serwisowe o następujących cechach:

1. Wsparcie serwisowe świadczone w siedzibie Zamawiającego lub zdalnie przez okres minimum 12 miesięcy.
2. Wsparcie obejmuje:
    a. Sprzęt
    b. Oprogramowanie wbudowane i oprogramowanie narzędziowe zainstalowane na sprzęcie lub niezbędne do jego poprawnego funkcjonowania
3. Okno czasowe zgłaszania incydentów dotyczących sprzętu - 8 godzin, przez 5 dni w tygodniu,
4. Obsługa zgłoszeń w języku polskim;
5. Czas reakcji na incydenty dotyczące sprzętu – 4 godziny,
6. Powołujemy opiekuna po stronie Wykonawcy, którego zadaniem będzie koordynacja prac świadczonych na rzecz Zamawiającego
7. Imię i nazwisko, nr telefonu, adres e-mail opiekuna:
   ……..……
8. Zapewniamy dostęp do poprawek i nowych wersji oprogramowania objętego kontraktem serwisowym
9. Zapewniamy dostęp wyznaczonych osób Zamawiającego do baz wiedzy, zarówno producenta sprzętu, jak i oprogramowania,
10. Zobowiązujemy się na życzenie co najmniej 2 razy w roku dostarczać pisemne rekomendacje (dopuszczalna jest forma przekazania informacji drogą elektroniczną) odnośnie instalacji nowych wersji oprogramowania wbudowanego (mikrokody) i sterowników urządzeń (device driver);
11. Zobowiązujemy się na życzenie co najmniej 2 razy w roku dostarczać pisemne rekomendacje (dopuszczalna jest forma przekazania informacji drogą elektroniczną) odnośnie instalacji poprawek do oprogramowania objętego serwisem
12. Zobowiązujemy się na życzenie przeprowadzić raz na pół roku przegląd techniczny urządzenia obejmujący:
    a. Weryfikację poprawności funkcjonowania sprzętu;
    b. Instalację rekomendowanych nowych wersji mikrokodów i sterowników urządzeń;
    c. Instalację rekomendowanych poprawek do systemu operacyjnego i oprogramowania narzędziowego

Podpisano
(upoważniony przedstawiciel oferenta)

Załącznik nr 7

Szczegółowy opis przedmiotu zamówienia

Platforma sprzętowa TYP A: 2 sztuki
Producent:……..
Model/Typ: ……...

Lp.	Parametr	Wymagania techniczne
1.	Architektura systemu ochrony	Urządzenie nie może posiadać twardego dysku, w zamian używać pamięci FLASH. Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizowanego 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, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie).
2.	System operacyjny	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.
3.	Ilość/rodzaj portów	Nie mniej niż 10 portów Ethernet 10/100/1000 Base-TX oraz 8 porty SFP.
4.	Funkcjonalności podstawowe i uzupełniające	System ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych: • kontrolę dostępu - zaporę ogniową klasy Stateful Inspection • ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, IM, SMTPS, POP3S, IMAPS, HTTPS) • poufność danych - IPSec VPN oraz SSL VPN • ochronę przed atakami - Intrusion Prevention System [IPS/IDS] oraz funkcjonalności uzupełniających: • kontrolę treści – Web Filter [WF] • kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) • kontrolę pasma oraz ruchu [QoS i Traffic shaping] • kontrolę aplikacji (wsparcie dla co najmniej tysiąca aplikacji w tym IM oraz P2P) • zapobieganie przed wyciekiem informacji poufnej DLP (Data Leak Prevention)
5.	Zasada działania (tryby)	Urządzenie powinno dawać możliwość ustawienia jednego z dwóch trybów pracy: • jako router/NAT (3.warstwa ISO-OSI) lub • jako 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 sieci, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem (m.in. pasmo gwarantowane i maksymalne, priorytety, oznaczenia DiffServ).
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). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP. • Nie mniej niż 4000 sygnatur ataków. • Aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie • 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 bez dodatkowych licencji nie mniej niż 10 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne ustawienia wszystkich funkcji bezpieczeństwa i dostęp administracyjny. 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.	Połączenia VPN	Wymagane nie mniej niż: • Tworzenie połączeń w topologii Site-to-site oraz Client-to-site • Dostawca musi udostępniać klienta VPN własnej produkcji realizującego następujące mechanizmy ochrony końcówki: o firewall o antywirus o web filtering o antyspam • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności • Konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu (interface based VPN) • Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
11.	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 • haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP • haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych Rozwiązanie powinno umożliwiać budowę logowania Single Sign On w środowisku Active Directory oraz eDirectory bez dodatkowych opłat licencyjnych.
12.	Wydajność	Obsługa nie mniej niż 6 000 000 jednoczesnych połączeń i 280 000 nowych połączeń na sekundę Przepływność nie mniejsza niż 16 Gbps dla ruchu nieszyfrowanego i 14 Gbps dla VPN (3DES). Obsługa nie mniej niż 2 000 jednoczesnych tuneli VPN
13.	Funkcjonalność zapewniająca niezawodność	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive

14.	Konfiguracja i zarządzanie	Możliwość konfiguracji poprzez terminal i linię komend oraz wbudowaną 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. Jednocześnie, dla systemu bezpieczeństwa powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta.
15.	Zarządzanie	System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem centralnego zarządzania umożliwiającm: • Przechowywanie i implementację polityk bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej • Wersjonowanie polityk w taki sposób aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości • Zarządzanie wersjami firmware'u na urządzeniach oraz zdalne uaktualnienia • Zarządzenie wersjami baz sygnatur na urządzeniach oraz zdalne uaktualnienia • Monitorowanie w czasie rzeczywistym stanu urządzeń (użycie CPU, RAM) • Zapis i zdalne wykonywanie skryptów na urządzeniach
16.	Raportowanie	System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem raportowania i korelacji logów umożliwiającym: • Zbieranie logów z urządzeń bezpieczeństwa • Generowanie raportów • Skanowanie podatności stacji w sieci • Zdalną kwarantannę dla modułu antywirusowego
17.	Integracja systemu zarządzania	Zgodnie z zaleceniami normy PN-ISO/17799 zarówno moduł centralnego zarządzania jak i raportowania muszą być zrealizowane na osobnych urządzeniach sprzętowych lub wirtualnych. Jednocześnie administrator powinien mieć do dyspozycji jedną konsolę zarządzającą do kontroli obu podsystemów.
18.	Serwis oraz aktualizacje	Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres jednego roku. System powinien być objęty serwisem gwarancyjnym producenta przez okres jednego roku.
19.	Wdrożenie i instalacja	Instalacja i konfiguracja systemu powinna być przeprowadzona przez uprawnionych inżynierów posiadających aktualny certyfikat producenta.
20.	Wsparcie techniczne	Dostawca powinien zapewnić pierwszą linie wsparcia technicznego telefonicznie w języku polskim w trybie 8 godzin 5 dni w tygodniu.

Platforma sprzętowa TYP B: 5 sztuk
Producent:……..
Model/Typ: ……...

Lp.	Parametr	Wymagania techniczne
1.	Architektura systemu ochrony	Urządzenie nie może posiadać twardego dysku, w zamian używać pamięci FLASH. Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizowanego 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, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie).
2.	System operacyjny	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.
3.	Ilość/rodzaj portów	Nie mniej niż 10 portów Ethernet 10/100/1000 Base-TX .
4.	Funkcjonalności podstawowe i uzupełniające	System ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych: • kontrolę dostępu - zaporę ogniową klasy Stateful Inspection • ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, IM) • poufność danych - IPSec VPN oraz SSL VPN • ochronę przed atakami - Intrusion Prevention System [IPS/IDS] oraz funkcjonalności uzupełniających: • kontrolę treści – Web Filter [WF] • kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) • kontrolę pasma oraz ruchu [QoS i Traffic shaping] • kontrolę aplikacji (wsparcie dla co najmniej tysiąca aplikacji w tym IM oraz P2P) • zapobieganie przed wyciekiem informacji poufnej DLP (Data Leak Prevention)
5.	Zasada działania (tryby)	Urządzenie powinno dawać możliwość ustawienia jednego z dwóch trybów pracy: • jako router/NAT (3.warstwa ISO-OSI) lub • jako 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 sieci, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem (m.in. pasmo gwarantowane i maksymalne, priorytety, oznaczenia DiffServ).

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). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP. • Nie mniej niż 4000 sygnatur ataków. • Aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie • 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 bez dodatkowych licencji nie mniej niż 10 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne ustawienia wszystkich funkcji bezpieczeństwa i dostęp administracyjny. 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.	Połączenia VPN	Wymagane nie mniej niż: • Tworzenie połączeń w topologii Site-to-site oraz Client-to-site • Dostawca musi udostępniać klienta VPN własnej produkcji realizującego następujące mechanizmy ochrony końcówki: o firewall o antywirus o web filtering o antyspam • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności • Konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu (interface based VPN) • Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
11.	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 • haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP • haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych Rozwiązanie powinno umożliwiać budowę logowania Single Sign On w środowisku Active Directory oraz eDirectory bez dodatkowych opłat licencyjnych.
12.	Wydajność	Obsługa nie mniej niż 500 000 jednoczesnych połączeń i 4 000 nowych połączeń na sekundę Przepływność nie mniejsza niż 1.5 Gbps dla ruchu nieszyfrowanego i 1 Gbps dla VPN (3DES). Obsługa nie mniej niż 200 jednoczesnych tuneli VPN
13.	Funkcjonalność zapewniająca niezawodność	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive

14.	Konfiguracja i zarządzanie	Możliwość konfiguracji poprzez terminal i linię komend oraz wbudowaną 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. Jednocześnie, dla systemu bezpieczeństwa powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta.
15.	Zarządzanie	System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem centralnego zarządzania umożliwiającm: • Przechowywanie i implementację polityk bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej • Wersjonowanie polityk w taki sposób aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości • Zarządzanie wersjami firmware'u na urządzeniach oraz zdalne uaktualnienia • Zarządzenie wersjami baz sygnatur na urządzeniach oraz zdalne uaktualnienia • Monitorowanie w czasie rzeczywistym stanu urządzeń (użycie CPU, RAM) • Zapis i zdalne wykonywanie skryptów na urządzeniach
16.	Raportowanie	System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem raportowania i korelacji logów umożliwiającym: • Zbieranie logów z urządzeń bezpieczeństwa • Generowanie raportów • Skanowanie podatności stacji w sieci • Zdalną kwarantannę dla modułu antywirusowego
17.	Integracja systemu zarządzania	Zgodnie z zaleceniami normy PN-ISO/17799 zarówno moduł centralnego zarządzania jak i raportowania muszą być zrealizowane na osobnych urządzeniach sprzętowych. Jednocześnie administrator powinien mieć do dyspozycji jedną konsolę zarządzającą do kontroli obu podsystemów.
18.	Serwis oraz aktualizacje	System powinien być objęty serwisem gwarancyjnym producenta przez okres jednego roku.
19.	Wdrożenie i instalacja	Instalacja i konfiguracja systemu powinna być przeprowadzona przez uprawnionego inżyniera posiadającego aktualny certyfikat producenta.
20.	Wsparcie techniczne	Dostawca powinien zapewnić pierwszą linie wsparcia technicznego telefonicznie w języku polskim w trybie 8 godzin 5 dni w tygtodniu.

Platforma do zarządzania: 1 sztuka
Producent:……..
Model/Typ: ……...

Lp.	Parametr	Wymagania techniczne
1.	Architektura systemu	System centralnego zarządzania powinien stanowić centralny punkt, w którym definiowana jest polityka bezpieczeństwa dla całej implementowanej infrastruktury bezpieczeństwa obejmującej urządzenia sieciowe. Powinien zostać dostarczony w postaci dedykowanej platformy programowej dla środowiska VMware ESXi / ESX min. 5.0
2.	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności system musi być dedykowanym systemem operacyjnym wzmocnionym z punktu widzenia bezpieczeństwa. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia.
3.	Parametry systemu	Obsługa nie mniej niż 4 wirtualnych interfejsów sieciowych Obsługiwana powierzchnia dyskowa powinna wynosić co najmniej 1TB, zaś obsługiwana liczba logów powinna wynosić co najmniej 10 GB na dzień .
4.	Funkcjonalności podstawowe i uzupełniające	System musi zapewniać: • Pełną konfigurację urządzeń, ze wszystkimi ich funkcjami składowymi • Przechowywanie i implementację polityk bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej • Wersjonowanie polityk w taki sposób aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości • Zarządzanie wersjami firmware'u na urządzeniach oraz zdalne uaktualnienia • Zarządzenie wersjami baz sygnatur na urządzeniach oraz zdalne uaktualnienia • Monitorowanie w czasie rzeczywistym stanu urządzeń (użycie CPU, RAM) • Zapis i zdalne wykonywanie skryptów na urządzeniach • Automatyzację procesu konfiguracji struktur VPN typu hub-and-spoke oraz full-mash
5.	Parametry wydajnościowe	Urządzenie musi obsługiwać: • Do 60 urządzeń sieciowych
6.	Sygnatury, subscrypcje	System musi zapewniać: • Lokalną bazę kontentu dla realizowanych funkcji bezpieczeństwa (IPS, AV, WF, AS) • Planowanie aktualizacji bazy szczepionek i sygnatur w czasie (Scheduler)
7.	Zarządzanie	System udostępnia: • Lokalny interfejs zarządzania poprzez szyfrowane połączenie HTTPS, SSH
8.	Serwis oraz aktualizacje	System powinien być objęty serwisem gwarancyjnym producenta przez okres jednego roku.

1. Wdrożenie

a. W ramach wdrożenia Wykonawca przygotuje projekt techniczny obejmujący zmianę topologii sieci Zamawiającego, dokona konfiguracji dostarczanych urządzeń oraz niezbędnej na potrzeby wdrożenia rekonfiguracji urządzeń posiadanych przez Zamawiającego, a także sporządzi dokumentację powykonawczą.

b. Prace wdrożeniowe, które wymagają przerwy w działaniu sieci bądź serwerów Zmawiającego można wykonywać tylko poza godzinami pracy Zamawiającego tj. w soboty i niedziele lub po godz. 16 w dni robocze.

2. Gwarancja i wsparcie

a. Zamawiający wymaga dostępu do pobierania nowych wersji oprogramowania oraz jego aktualizacji, dostępu /do narzędzi diagnostycznych oraz do bazy wiedzy producenta.

b. Zamawiający dopuszcza zastosowanie przez wykonawców rozwiązań równoważnych rozwiązaniom opisywanym w niniejszej specyfikacji istotnych warunków zamówienia.

c. Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by były nieużywane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem). Przy dostawie Wykonawca musi dostarczyć oświadczenie wykonawcy zawierające miesiąc oraz rok produkcji dostarczonego sprzętu.

d. Wykonawca, który w ofercie powoła się na zastosowanie rozwiązań równoważnych jest obowiązany wykazać, że oferowane przez niego urządzenia spełniają wymagania określone przez zamawiającego

3. Warsztaty szkoleniowe

a. Wykonawca zobowiązuje się do przeprowadzenia na rzecz zamawiającego minimum 3-dniowe warsztaty szkoleniowe dla 2 osób. Tematyka szkolenia musi obejmować obsługę zamawianych urządzeń.
b. Warsztaty szkoleniowe muszą być przeprowadzone przez wykwalifikowanego inżyniera posiadającego aktualny certyfikat producenta zamawianych urządzeń.
c. W przypadku warsztatów poza Lublinem Wykonawca pokryje koszty zakwaterowania uczestników.

Załącznik nr 8

Projekt umowy

zawarta w dniu
pomiędzy

§ 1

W wyniku przeprowadzenia przetargu nieograniczonego Zamawiający zleca, a Wykonawca zobowiązuje się do modernizacji infrastruktury sieci WAN, zgodnie ze specyfikacją istotnych warunków zamówienia i ofertą Wykonawcy z dnia ..... stanowiącą załącznik nr ..... do niniejszej umowy.

§ 2

Wynagrodzenie z tytułu realizacji przedmiotu umowy wynosi: Netto: ..... zł (słownie: .....) Podatek VAT: ..... zł (słownie: .....) Brutto: ..... zł (słownie: .....) zgodnie z kosztorysem ofertowym.

§ 3

1. Strony ustalają termin realizacji zamówienia do dnia ..... .

§ 4

1. Wykonawca na dokonaną modernizację infrastruktury sieci WAN, dostarczone urządzenia i materiały udziela gwarancji na okres określony w formularzu kosztorysu ofertowego liczony od dnia podpisania protokołu zdawczo-odbiorczego.
2. Zamawiającemu, niezależnie od uprawnień z tytułu gwarancji, określonych w niniejszej umowie, przysługują uprawnienia z tytułu rękojmi.
3. W przypadku ujawnienia się w okresie gwarancji wad fizycznych Sprzętu lub zużycia świadczącego o niższej jakości niż zapewniana, Wykonawca zobowiązuje się do nieodpłatnego usunięcia tych wad w terminie wyznaczonym przez zamawiającego poprzez naprawę Sprzętu lub wymianę elementów, które uległy pogorszeniu.
4. Warunki usług gwarancyjnych i wsparcia serwisowego określa załącznik nr ..... .

§ 5

Wykonawca oświadcza, że sprzedany, dostarczony i zainstalowany Sprzęt nie posiada wad fizycznych, ani prawnych i jest najwyższej jakości oraz zobowiązuje się wykonać całość prac zgodnie z obowiązującymi przepisami prawa.

§ 6

1. Rozliczenie wynagrodzenia z tytułu realizacji umowy nastąpi w oparciu o fakturę VAT wystawioną po podpisaniu przez upoważnionych przedstawicieli stron protokołu odbioru.

2. Zamawiający dokona płatności faktury w formie przelewu na rachunek Wykonawcy wskazany na fakturze w ciągu 21 dni od daty otrzymania faktury wystawionej po realizacji zamówienia.
3. Zamawiający upoważnia Wykonawcę do wystawiania faktur VAT bez podpisu Zamawiającego.
4. Faktury powinna zawierać następujące dane:

Nabywca	Odbiorca i płatnik dowodu:
Narodowy Fundusz Zdrowia w Warszawie	Lubelski Oddział Wojewódzki w Lublinie
ul. Grójecka 186, 02-390 Warszawa	ul. Szkolna 16, 20-124 Lublin
NIP 1070001057	

5. Strony przyjmują, że za dzień dokonania zapłaty uważają datę obciążenia rachunku bankowego Zamawiającego.

§ 7

Każda ze stron może odstąpić od umowy w terminie 14 dni od daty stwierdzenia nienależytego jej wykonania lub wykonania w sposób sprzeczny z ofertą lub specyfikacją istotnych warunków zamówienia.

§ 8

1. Wykonawca zapłaci Zamawiającemu karę umowną:
   1) za odstąpienie od umowy przez Zamawiającego z przyczyn, o których mowa w § 7 w wysokości 5% wartości umowy brutto określonej w § 2,
   2) za zwłokę w dostawie w wysokości 0,5% wartości umowy brutto określonej w § 2, za każdy dzień zwłoki,
   3) za zwłokę w usunięciu wad stwierdzonych przy odbiorze, w wysokości 0,5% wartości umowy brutto określonej w § 2 za każdy dzień zwłoki liczony od dnia wyznaczonego na usunięcie wad.
   4) za nieterminową naprawę Sprzętu w wysokości 500 zł brutto za każdy dzień opóźnienia po dniu ustalonym jako termin naprawy.
2. Wykonawca może obciążyć Zamawiającego odsetkami ustawowymi w przypadku zwłoki w dokonaniu zapłaty należności.
3. Strony mają prawo dochodzić odszkodowania uzupełniającego na zasadach Kodeksu Cywilnego, jeżeli szkoda przewyższa wartość kar umownych.

§ 9

1. Zamawiający wyznacza do nadzorowania prac związanych z realizacją niniejszej umowy oraz od podpisania protokołu odbioru następujące osoby:
……

2. Wykonawca wyznacza do nadzorowania prac związanych z realizacją niniejszej umowy oraz od podpisania protokołu odbioru następujące osoby:
……..
3. Osoby wskazane w ust. 1 i 2 są uprawnione do wykonywania wszelkich czynności niezbędnych do prawidłowej i zgodnej z umową realizacji przedmiotu zamówienia, ustalania harmonogramów realizacji zamówienia oraz podpisywania protokołów odbioru.

§ 10

1. Strony oświadczają, że będą dążyć aby wszelkie ewentualne spory odnośnie treści lub wykonania umowy uzgadniać polubownie. Jeżeli rozwiązanie polubowne nie będzie możliwe, spór zostanie rozstrzygnięty przez właściwy sąd w Lublinie.
2. Wszelkie ustalenia związane z niniejszą umową strony będą przyjmowały w formie pisemnej, w postaci protokołów uzgodnień.
3. W sprawach nieuregulowanych niniejszą umową stosuje się przepisy ustawy z dnia 29 stycznia 2004 r. prawo zamówień publicznych oraz Kodeksu Cywilnego
4. Umowa została sporządzona w trzech jednobrzmiących egzemplarzach, dwa dla Zamawiającego, jeden dla Wykonawcy.

Wykonawca Zamawiający