

## SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

### 1. NAZWA I ADRES ZAMAWIAJĄCEGO

Narodowy Fundusz Zdrowia Centrala (w skrócie NFZ) ,  
ul. Grójecka 186,  
02-390 Warszawa.

### 2. TRYB UDZIELENIA ZAMÓWIENIA

Postępowanie jest prowadzone w trybie przetargu nieograniczonego, zgodnie z przepisami ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity Dz. U. z 2010, Nr 113, poz. 759), zwanej dalej ustawą.

### 3. OPIS PRZEDMIOTU ZAMÓWIENIA

- 3.1. Przedmiotem zamówienia jest „**Wdrożenie systemu monitorowania bezpieczeństwa w środowisku systemów informatycznych NFZ**”. **Przez wdrożenie systemu monitorowania bezpieczeństwa w NFZ Zamawiający rozumie dostawę licencji, dostawę urządzeń, zaprojektowanie systemu oraz jego uruchomienie, a także przeprowadzenie warsztatów.** Szczegółowy opis przedmiotu zamówienia stanowi załącznik nr 1 do Specyfikacji Istotnych Warunków Zamówienia zwaną dalej „Specyfikacją”.
- 3.2. Szczegółowy zakres praw i obowiązków związanych z realizacją zamówienia określa wzór umowy określony w załączniku nr 2 do Specyfikacji.
- 3.3. Zamawiający dopuszcza udział podwykonawców w wykonaniu zamówienia. W przypadku wykonywania części zamówienia przez podwykonawcę Wykonawca wskaże w formularzu ofertowym, stanowiącym załącznik nr 3 do Specyfikacji, część zamówienia, które powierza podwykonawcy.
- 3.4. Zamawiający nie dopuszcza składania ofert częściowych oraz wariantowych.

### 4. TERMIN WYKONANIA ZAMÓWIENIA

Zamawiający wymaga, aby zamówienie zostało zrealizowane w ciągu 20 tygodni od dnia podpisania umowy.

### 5. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ OPIS SPOSOBU DOKONYWANIA OCENY SPEŁNIANIA TYCH WARUNKÓW

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu z postępowania o udzielenie zamówienia publicznego na podstawie art. 24 ust. 1 ustawy oraz spełniają warunki udziału w postępowaniu określone w art. 22 ust. 1 ustawy dotyczące:

- 1) posiadania uprawnień do wykonania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania,
- 2) posiadania wiedzy i doświadczenia,

*opis sposobu dokonywania oceny spełniania tego warunku*

- wykażą się, że wykonali (a w przypadku świadczeń okresowych lub ciągłych uwzględniane są również wykonywane) w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, co najmniej 3 dostawy **polegające na wdrożeniu systemu monitorowania bezpieczeństwa w środowisku systemów informatycznych, każda o wartości przekraczającej 200.000,00 zł brutto** z podaniem ich wartości, przedmiotu, dat wykonania i odbiorców oraz załączenia dokumentów potwierdzających, że dostawy te zostały wykonane lub są wykonywane należycie.

- 3) dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonywania zamówienia,
- 4) sytuacji ekonomicznej i finansowej.

Ocena spełniania warunków zostanie dokonana według formuły „spełnia” / „nie spełnia” warunków udziału w postępowaniu w oparciu o informacje zawarte w dokumentach i oświadczeniach zawartych w pkt 6 Specyfikacji. Nie spełnienie warunków udziału w postępowaniu skutkować będzie wykluczeniem Wykonawcy z postępowania.

*Jeżeli Wykonawcy wykazują spełnianie powyższych warunków polegając na zasobach innych podmiotów na zasadach określonych w art. 26 ust.2b ustawy, a podmioty te będą brały udział w realizacji części zamówienia, zamawiający może żądać od Wykonawcy przedstawienia w odniesieniu do tych podmiotów dokumentów, o których mowa w pkt.6*

## **6. WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW, JAKIE MAJĄ DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU**

### **6.1. W celu potwierdzenia spełniania warunków udziału w postępowaniu Wykonawca zobowiązany jest załączyć do oferty następujące dokumenty i oświadczenia:**

**6.1.1. Oświadczenie o spełnianiu warunków udziału w postępowaniu** zgodnie z załącznikiem nr 4 do Specyfikacji.

**6.1.2. Wykaz wykonanych dostaw wraz z dokumentami, że dostawy te zostały wykonane należyście.**

Wykonawca zobowiązany jest przedstawić pisemny wykaz wykonanych (a w przypadku świadczeń okresowych lub ciągłych uwzględniane są również wykonywane) w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, co najmniej 3 dostaw, **polegających na wdrożeniu systemu monitorowania bezpieczeństwa w środowisku systemów informatycznych, każda o wartości przekraczającej 200.000,00 zł brutto**, z podaniem ich wartości, przedmiotu, data wykonania i odbiorców oraz załączenia dokumentów potwierdzających, że dostawy te zostały wykonane lub są wykonywane należyście.

Wzór wykazu stanowi załącznik nr 6 do Specyfikacji.

W przypadku składania oferty przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, wyżej wymieniony warunek musi spełniać co najmniej 1 podmiot lub warunek podmioty te mogą spełniać łącznie.

*Jeżeli Wykonawca wykazując spełnianie warunków, o których mowa w pkt 5.2 Specyfikacji, polega na zasobach innych podmiotów na zasadach określonych w art. 26 ust. 2b ustawy, a podmioty te będą brały udział w realizacji części zamówienia, Zamawiający żąda od Wykonawcy przedstawienia w odniesieniu do tych podmiotów dokumentów wymienionych w punkcie 6.2 Specyfikacji.*

### **6.2. W celu wykazania braku podstaw do wykluczenia z postępowania o udzielenie zamówienia Wykonawca zobowiązany jest załączyć do oferty następujące dokumenty i oświadczenia:**

**6.2.1. Oświadczenie o braku podstaw do wykluczenia** zgodnie z załącznikiem nr 5 do Specyfikacji.

**6.2.2. Aktualny odpis z właściwego rejestru**, jeżeli odrębne przepisy wymagają wpisu do rejestru, w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust.1 pkt 2 ustawy, wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert, a w stosunku do osób fizycznych oświadczenie Wykonawcy w zakresie art. 24 ust.1 pkt 2 ustawy.

**6.2.3. Wykonawcy zagraniczni**

1. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentu, o którym mowa w pkt 6.2.2, 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. Dokumenty powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

2. Jeżeli w kraju pochodzenia osoby lub w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w pkt 1, zastępuje je się 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. Dokumenty powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

#### **6.2.4. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia**

1. 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 poświadczony notarialnie za zgodność z oryginałem kopii.
2. Wykonawcy, o których mowa w pkt 1., składają jedną ofertę, przy czym:
  - a) wymagane oświadczenia lub dokumenty wskazane w pkt 6.2.1 i 6.2.2 składa osobno każdy z Wykonawców,
  - b) warunek określony w pkt 5 ppkt 2 musi spełniać co najmniej 1 podmiot lub warunek podmioty te mogą spełniać łącznie,
  - c) załączone do oferty dokumenty muszą być przedłożone w formie oryginałów bądź kserokopii poświadczonych „za zgodność z oryginałem” przez wykonawcę na każdej zapisanej stronie kserowanego dokumentu. Poświadczenie „za zgodność z oryginałem” musi zostać sporządzone przez osoby uprawnione do reprezentowania Wykonawcy - wskazane we właściwym rejestrze lub ewidencji działalności gospodarczej. Podpisy złożone przez Wykonawcę powinny być opatrzone czytelnym imieniem i nazwiskiem lub pieczęcią imienną. Uwaga! każdy z Wykonawców poświadcza „za zgodność z oryginałem” dokumenty, które go dotyczą.

#### **7. INFORMACJA O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ LUB DOKUMENTÓW, A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI**

Zgodnie z art. 38 ustawy, Zamawiający jest obowiązany niezwłocznie udzielić wyjaśnień treści specyfikacji na zasadach określonych w art. 38 ust. 1 i 1b. Treść zapytań wraz z wyjaśnieniami (bez ujawniania źródła zapytania) Zamawiający przekazuje Wykonawcom, którym przekazał Specyfikację, a jeżeli Specyfikacja jest udostępniana na stronie internetowej - zamieszcza na tej stronie.

Zamawiający nie przewiduje zwołania zebrania Wykonawców w celu wyjaśnienia wątpliwości dotyczących treści Specyfikacji.

Zamawiający zastrzega, że zgodnie z art. 38 ust. 4 ustawy w uzasadnionych przypadkach może przed upływem terminu składania ofert zmienić treść specyfikacji. Dokonaną zmianę specyfikacji Zamawiający przekazuje

niezwłocznie wszystkim wykonawcom, którym przekazano Specyfikację, a jeżeli Specyfikacja jest udostępniana na stronie internetowej, zamieszcza ją także na tej stronie.

Oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują faksem lub drogą elektroniczną.

Nr faksu Zamawiającego : 022 572 -63-05. poczta: [anna.pawlak@nfz.gov.pl](mailto:anna.pawlak@nfz.gov.pl)

Zamawiający przekazywać będzie oświadczenia, wnioski, zawiadomienia oraz informacje faksem lub drogą elektroniczną i żąda niezwłocznego potwierdzenia przez Wykonawcę faktu ich otrzymania.

Uprawnionymi do porozumiewania się z wykonawcami pracownikami Zamawiającego są:

- 1) w sprawach dotyczących strony formalnej niniejszego postępowania:
  - Zbigniew Johne
- 2) w sprawach dotyczących przedmiotu zamówienia:
  - Robert Czarnecki

w dni robocze od poniedziałku do piątku, w godz. 09:00-15:00.

## **8. WYMAGANIA DOTYCZĄCE WADIUM**

Zamawiający nie wymaga wniesienia wadium .

## **9. TERMIN ZWIĄZANIA OFERTA**

Wykonawca jest związany treścią oferty przez okres 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą, z tym że Zamawiający może tylko raz , co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni.

## **10. OPIS SPOSOBU PRZYGOTOWANIA OFERT**

1. Oferta winna być sporządzona zgodnie z treścią formularza oferty załączonego do Specyfikacji. Wykonawca może złożyć ofertę na własnych formularzach, których treść musi być zgodna z formularzami załączonymi do Specyfikacji.
2. **Ofertę** (wypełniony formularz oferty wraz z wymaganymi przez Specyfikację oświadczeniami) **muszą podpisać osoby uprawnione** do reprezentowania Wykonawcy - wskazane we właściwym rejestrze lub ewidencji działalności gospodarczej. Ofertę podpisać może pełnomocnik wykonawcy, jeżeli do oferty zostanie załączone pełnomocnictwo do podejmowania określonych czynności, wynikających z ustawy Prawo zamówień publicznych, w postępowaniach o udzielenie zamówień publicznych, w których bierze udział wykonawca, albo szczególne dotyczące niniejszego postępowania. **Dokument pełnomocnictwa musi być złożony w oryginale lub poświadczony notarialnie za zgodność z oryginałem kopii.** Podpisy złożone przez Wykonawcę powinny być opatrzone czytelnym imieniem i nazwiskiem lub pieczęcią imienną.
3. **Załączone do oferty dokumenty** muszą być przedłożone w formie oryginałów bądź kserokopii poświadczonych „za zgodność z oryginałem” przez wykonawcę na każdej zapisanej stronie kserowanego dokumentu. Poświadczenie ”za zgodność z oryginałem” musi zostać sporządzone przez osoby uprawnione do reprezentowania Wykonawcy - wskazane we właściwym rejestrze lub ewidencji działalności gospodarczej **Podpisy złożone przez Wykonawcę powinny być opatrzone czytelnym imieniem i nazwiskiem lub pieczęcią imienną.** Uznaje się, że pełnomocnictwo do podpisania oferty obejmuje pełnomocnictwo do poświadczenia za zgodność z oryginałem kopii dokumentów załączanych do oferty. Zamawiający może żądać przedstawienia oryginału lub notarialnie poświadczonej kopii wyłącznie wtedy, gdy złożona przez Wykonawcę kopia dokumentu jest nieczytelna lub budzi wątpliwości co do jej prawdziwości.  
Uwaga! każdy z Wykonawców poświadcza ”za zgodność z oryginałem” dokumenty, które go dotyczą.
4. Każdy Wykonawca może złożyć jedną ofertę. Złożenie większej liczby ofert spowoduje odrzucenie wszystkich ofert złożonych przez danego Wykonawcę.

5. Ofertę składa się pod rygorem nieważności w formie pisemnej. Zamawiający nie wyraża zgody na złożenie oferty w postaci elektronicznej.
6. Treść oferty musi odpowiadać treści Specyfikacji.
7. Oferta musi być sporządzona w języku polskim, na komputerze lub inna trwałą i czytelną techniką. Poprawki lub zmiany w ofercie muszą być dokonane w sposób czytelny i parafowane przez osobę podpisującą ofertę.
8. Zaleca się aby oferta wraz z załączonymi do oferty oświadczeniami i dokumentami była zszyta lub spięta (np. zbindowana) i posiadała ponumerowane strony.
9. Dokumenty sporządzone w języku obcym muszą być złożone wraz z tłumaczeniem na język polski, poświadczonym przez wykonawcę.
10. Jeżeli oferta zawiera informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji powinny one być umieszczone w osobnej wewnętrznej kopercie zatytułowanej „Dostawa systemu monitorowania bezpieczeństwa w środowisku systemów informatycznych NFZ”. Tajemnica przedsiębiorstwa”.
11. Sporządzoną ofertę należy opakować w kopertę oznaczoną dokładną nazwą i adresem wykonawcy oraz napisem „POSTĘPOWANIE NR AZP – 2611 - 14/10. OFERTA – „Dostawa systemu monitorowania bezpieczeństwa w środowisku systemów informatycznych NFZ”. NIE OTWIERAĆ PRZED 06.09.2010 r. GODZ. 10:30.”.
12. **Wykonawca zobowiązany jest załączyć do oferty następujące dokumenty:**
  - Wykaz charakterystyki funkcjonalnej oferowanego produktu w ujęciu całościowym oraz w rozbiciu na moduły funkcjonalne, której wzór stanowi załącznik nr 8 do SIWZ
  - Wykaz oferowanych stacji monitorujących- stanowi załącznik nr 9 do SIWZ,
  - Oświadczenie o poszczególnych cenach jednostkowych stacji monitorujących, którego wzór stanowi załącznik nr 10 do SIWZ,
  - Oświadczenie o poszczególnych cenach jednostkowych licencji, którego wzór stanowi załącznik nr 11 do SIWZ,

## **11. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT**

1. Oferty należy składać w zamkniętych kopertach w Centrali Narodowego Funduszu Zdrowia w Warszawie, przy ul. Grójeckiej 186, 02-390 Warszawa, I p., pok. 1.14, **w terminie do dnia 06.09.2010 r. do godz. 10:00.**
2. Złożona oferta zostanie zarejestrowana w ten sposób, że osoba przyjmująca oznaczy kopertę kolejnym numerem oraz odnotuje datę i dokładny czas wpływu. Na żądanie Wykonawcy zostanie wydany dowód wpływu oferty, zawierający odcisk pieczęci organizatora postępowania, nazwisko i imię osoby przyjmującej, oznaczenie postępowania oraz datę i dokładny czas wpływu.
3. Jeżeli oferta jest wysyłana za pomocą przesyłki kurierskiej/listowej, Wykonawca winien zaznaczyć, że przesyłka zawiera ofertę oraz wskazać numer postępowania. Zamawiający nie ponosi odpowiedzialności za następstwa spowodowane brakiem zabezpieczenia oferty lub brakiem którejkolwiek z ww. informacji.
4. Zamawiający zastrzega, że wyłączne ryzyko nieterminowego dostarczenia oferty oraz pomyłkowego otwarcia wskutek nienależytego oznaczenia koperty ponosi wykonawca.
5. Przed upływem terminu składania ofert, Wykonawca może wycofać ofertę lub wprowadzić zmiany do złożonej oferty. Informacja o wycofaniu oferty lub zmiany do oferty Wykonawca winien doręczyć Zamawiającemu na piśmie przed upływem terminu składania ofert. Oświadczenie o wycofaniu oferty lub wprowadzeniu zmian w ofercie winno być opakowane tak jak oferta, a opakowanie winno być dodatkowo oznaczone odpowiednio wyrazem „WYCOFANIE” lub „ZMIANA”. Opakowania te będą otwierane w terminie otwarcia ofert, określonym w niniejszej specyfikacji. Koperty oznakowane „WYCOFANIE” będą otwierane w pierwszej kolejności. Po stwierdzeniu poprawności postępowania Wykonawcy, oferty wycofane nie będą otwierane.
6. Otwarcie ofert odbędzie się **w dniu 06.09.2010 r. o godz. 10:30** w Centrali Narodowego Funduszu Zdrowia w Warszawie przy ul. Grójeckiej 186, I p., pok. 1.14.

## **12. OPIS SPOSOBU OBLICZENIA CENY**

Zamawiający wymaga, by oferowana cena za realizację przedmiotu zamówienia została wyliczona zgodnie z formułą określoną w formularzu ofertowym. Jako podstawę do oceny ofert Zamawiający przyjmuje cenę brutto (z podatkiem od towarów i usług VAT) za realizację zamówienia.

### **UWAGA!**

Zamawiający wymaga, by oferowana cena została przedstawiona w rozbiciu na:

cenę netto, podatek od towarów i usług (VAT) oraz cenę brutto –cenę tę można podać z dokładnością do setnych części grosza.

Jako podstawę do oceny ofert Zamawiający przyjmuje łączną cenę brutto, która w toku postępowania nie może ulec zmianie.

Wszystkie ceny powinny zawierać w sobie ewentualne upusty proponowane przez Wykonawcę (niedopuszczalne są żadne negocjacje cenowe).

Wszelkie rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w PLN.

### **13. OCENA OFERT**

Do oceny ofert zakwalifikowanych jako ważne Zamawiający przyjął kryterium określone w ogłoszeniu o zamówieniu wraz ze wskazaniem jego znaczenia (wagą wyrażoną w % udziale w ocenie oferty).

Zaokrąglenia w obliczeniach końcowych punktacji – do dwóch miejsc po przecinku.

Szczegółowe zasady oceny z tytułu kryterium zostały przedstawione poniżej.

#### **13.1 Kryterium: CENA (100% wagi oceny)**

Z tytułu niniejszego kryterium maksymalna ilość punktów wynosi 100.

Oferta o najkorzystniejszej (najniższej) cenie brutto uzyska 100 pkt. Pozostałe ceny obliczone dla badanych ofert zostaną porównane z ofertą o najkorzystniejszej (najniższej) cenie brutto, stosując poniższy wzór:

$$K_m = \frac{C_n}{C_m} \times 100 \text{ pkt}$$

Gdzie:  $m$  – oznacza kolejną badaną ofertę,  
 $K_m$  – oznacza wynik oceny kolejnej badanej oferty w zakresie kryterium ceny,  
 $C_n$  – oznacza najkorzystniejszą (najniższą) cenę brutto badanej oferty,  
 $C_m$  – oznacza cenę brutto kolejnej badanej oferty.

#### **13.2 Ocena łączna**

Dla każdej oferty wyniki oceny z tytułu kryterium zostaną obliczone według poniższego wzoru.

$$O = K_m \times X \times W_c$$

Gdzie:  $O$  – oznacza ocenę łączną oferty  
 $K_m$  – oznacza wynik oceny kolejnej badanej oferty w zakresie kryterium ceny,  
 $X$  – oznacza niezmienną liczbę członków Komisji przetargowej biorących udział w ocenie,  
 $W_c$  - oznacza wagę oceny kryterium.

Zamawiający wybierze ofertę, która uzyska najwyższą ilość punktów zgodnie z powyższym wzorem.

### **14. INFORMACJE O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO**

Treść umowy o realizację zamówienia zostanie ustalona zgodnie z treścią wybranej oferty i załączonego do Specyfikacji wzoru umowy.

Zamawiający zawrze umowę w terminie nie krótszym niż 5 dni od dnia przekazania zawiadomienia o wyborze oferty, z zastrzeżeniem art. 94 ust. 2 ustawy.

W zawiadomieniu o wyborze oferty najkorzystniejszej Zamawiający poinformuje Wykonawcę o terminie i miejscu zawarcia umowy. Osoby reprezentujące Wykonawcę przy podpisywaniu umowy muszą posiadać ze sobą dokumenty potwierdzające ich umocowanie do podpisania umowy.

### **15. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY**

Wykonawca jest zobowiązany do wniesienia zabezpieczenia należytego wykonania umowy na sumę stanowiącą **10 %** ceny całkowitej /brutto/ podanej w ofercie.

Dopuszczalne są następujące formy zabezpieczenia:

1) w pieniądzu - wpłacane przelewem na konto bankowe Zamawiającego:

**77 1130 1017 0020 0734 8625 7421,**

2) w poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym, gwarancjach bankowych, gwarancjach ubezpieczeniowych, poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości.

**Zabezpieczenie może być wnoszone według wyboru Wykonawcy w jednej lub kilku formach.**

Kwoty pieniężne wpłacone tytułem zabezpieczenia Zamawiający przechowuje na oprocentowanym rachunku bankowym.

Zamawiający zwraca zabezpieczenie wniesione w pieniądzu z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszonymi o koszty prowadzenia tego rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy Wykonawcy.

Wykonawca jest obowiązany wnieść całość zabezpieczenia **najpóźniej w dniu podpisania umowy**. Zwrot zabezpieczenia nastąpi na warunkach określonych w umowie. Wadium wniesione w pieniądzu przez Wykonawcę, którego oferta została wybrana, za zgodą tego Wykonawcy zaliczane jest przez Zamawiającego na poczet zabezpieczenia należytego wykonania umowy. W trakcie realizacji umowy Wykonawca może dokonać zmiany formy zabezpieczenia, na jedną lub kilka form, o których mowa w pkt 1 i 2. Zmiana formy zabezpieczenia jest dokonywana z zachowaniem ciągłości zabezpieczenia i bez zmniejszenia jego wysokości

#### **16. WZÓR UMOWY – ZGODNIE Z ZAŁĄCZNIKIEM NR 2 DO SPECYFIKACJI**

#### **17. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA**

Wykonawcom a także innym osobom, których interes prawny, w uzyskaniu zamówienia, doznał lub może doznać uszczerbku, w wyniku naruszenia przez zamawiającego przepisów ustawy, przysługują środki ochrony prawnej określone w Dziale VI ustawy.

#### **Do Specyfikacji załączono:**

- 1) opis przedmiotu zamówienia (załącznik nr 1),
- 2) wzór umowy o wykonanie zamówienia (załącznik nr 2),
- 3) formularz oferty (załącznik nr 3),
- 4) formularz oświadczenia o spełnianiu warunków udziału w postępowaniu (załącznik nr 4),
- 5) formularz oświadczenia o braku podstaw do wykluczenia (załącznik nr 5),
- 6) formularz wykazu wykonanych dostaw (załącznik nr 6),
- 7) wykaz charakterystyki funkcjonalnej oferowanego produktu w ujęciu całościowym oraz w rozbiciu na moduły funkcjonalne (załącznik nr 7),
- 8) wykaz stacji monitorujących niezbędnych do wdrożenia oferowanego produktu (załącznik nr 8),
- 9) oświadczenie o poszczególnych cenach jednostkowych stacji monitorujących ( załącznik nr 9),
- 10) oświadczenie o poszczególnych cenach jednostkowych licencji( załącznik nr 10).

Po zawarciu umowy stanowić będzie załącznik nr 1 do umowy

## OPIS PRZEDMIOTU ZAMÓWIENIA

System monitorowania bezpieczeństwa (skrót SMB) – narzędzie pozwalające zespołom bezpieczeństwa na gromadzenie i analizowanie dużej ilości danych dotyczących zdarzeń związanych z systemami teleinformatycznymi. Rozwiązanie takie zbudowane w oparciu o narzędzie informatyczne klasy SIEM (ang. *Security Information and Event Management*) powinno pozwalać na zbieranie, normalizowanie, analizowanie i wizualizowanie w czasie rzeczywistym, danych z wszystkich urządzeń bezpieczeństwa i systemów teleinformatycznych działających u zamawiającego, a także pozwalać na raportowanie krótko - i długoterminowe.

Zaproponowane rozwiązanie powinno wspierać zespół monitorowania w procesie reakcji na wykryte incydenty bezpieczeństwa. System ma przetwarzać dane zarówno w celu bezpośredniego monitorowania bezpieczeństwa informacji jak i także w celu wspomagania procesu utrzymywania zgodności z regulacjami prawnymi i standardami bezpieczeństwa (tzw. *compliance*).

### Opis funkcjonalny systemu

Przez System Monitorowania Bezpieczeństwa (SMB), rozumiemy system który:

- Docelowo obejmuje monitorowaniem wszystkie krytyczne systemy informatyczne organizacji, rozumiane jako systemy wspierające najważniejsze procesy biznesowe
- Posiada informacje o użytkownikach systemów informatycznych i zdarzeniach w nich występujących w skali całej organizacji
- Posiada informacje o zasobach informatycznych organizacji, ich roli, krytyczności i innych parametrach istotnych do oceny ich ważności dla organizacji (kontekst biznesowy)
- Posiada narzędzia wspomagające analizowanie danych pochodzących z monitorowanych systemów
- Pozwala na podjęcie działań w odpowiedzi na zdarzenia niepożądane zanim przerodzą się w incydent
- Posiada narzędzia wspomagające proces reagowania na incydenty
- Dostarcza okresowe raporty i wskaźniki nt. zagrożeń, podatności, zdarzeń niepożądanych, incydentów i wynikających z tego ryzyk w skali całej organizacji

SMB o opisanych powyżej cechach składa się z trzech elementów:

- Zasobów ludzkich – personelu organizacji odpowiedzialnego za utrzymanie i eksploatację systemu, analizowanie informacji o zdarzeniach bezpieczeństwa, podejmowanie reakcji na incydenty i zdarzenia niepożądane oraz doskonalenie systemu.
- Procesów i procedur – które opisują i regulują sposób postępowania we wszystkich aspektach działania systemu.
- Narzędzi informatycznych – które mają za zadanie wspieranie procesów i personelu w realizacji zadań systemu.

SMB jest zasilany danymi pochodzącymi z monitorowanych systemów, dane te są poddawane analizie i na podstawie wyników analizy podejmowane są różnego rodzaju działania. Mogą to być działania o charakterze informacyjnym (np. wizualizacja zdarzeń, tworzenie raportów, powiadamianie osób odpowiedzialnych o zaistnieniu pewnych zdarzeń), reakcyjnym (np. rekonfiguracja urządzeń sieciowych, potrzeba zmian w polityce bezpieczeństwa systemu) lub modyfikacyjnym (potrzeba zmian w SMB). Najważniejszą cechą SMB, która decyduje o jego efektywności jest jakość analiz wykonywanych przez system.

Dane zasilające system pochodzą z systemów objętych monitorowaniem i nazywane są źródłami danych.

Dane napływające z systemów można podzielić na dwie główne kategorie:



- a) Zdarzenia – które opisują fakty, które można precyzyjnie umieścić w czasie i które są generowane przez monitorowane systemy w momencie zaistnienia danego faktu
- b) Pozostałe dane – które opisują fakty, których nie można precyzyjnie umieścić w czasie

Do pierwszej kategorii danych należy większość informacji przetwarzanych przez SMB (np. informacje o zalogowaniu się użytkownika do aplikacji, wystąpienie próby kompromitacji systemu - wykorzystania exploita itp.). Do drugiej kategorii danych należą informacje takie jak:

- a) Informacje o zasobach informatycznych i ich cechach.
- b) Informacje o konfiguracji systemów informatycznych.
- c) Informacje o stanie systemów informatycznych (np. aktualne obciążenie procesora, awaria zasilacza zapasowego).

Analiza danych zasilających SMB polega na przetwarzaniu informacji zdarzeniowych w kontekście informacji o stanie systemów monitorowanych (ich atrybutów/cech). Wynikiem tej analizy są działania podejmowane przez system. Sposób prowadzenia analizy określają procedury monitorowania oraz możliwości techniczne i konfiguracja narzędzi informatycznych stosowanych do wspierania analiz. Dla działań o charakterze modyfikacyjnym (zmiana konfiguracji systemów informatycznych organizacji) w praktyce zawsze konieczne jest podjęcie decyzji przez czynnik ludzki, ze względu na brak dostatecznie zaawansowanych technologii pozwalających na automatyczne podejmowanie decyzji w obszarze bezpieczeństwa. Personel wchodzący w skład SMB musi podjąć decyzję nie tylko o parametrach działania reakcyjnego ale także często wybrać samodzielnie najbardziej optymalny sposób działania w odpowiedzi na zaistniały incydent. Działania o charakterze modyfikacyjnym są również skomplikowane w obsłudze, gdyż modyfikacje systemów wymagają najczęściej formalnej ścieżki akceptacji zmian.

Propozycja powinna uwzględniać, pojedynczą konsolę, która umożliwi scentralizowane wykrywanie i odpowiadanie na naruszenia bezpieczeństwa w momencie ich zaistnienia. Ponadto zbierane dane w znormalizowanej postaci w jednym repozytorium danych, mają umożliwić zamawiającemu oprócz analiz w czasie rzeczywistym również wszelkie analizy historyczne.

Przedmiotem Zamówienia jest zaprojektowanie, dostarczenie i wdrożenie w oparciu o oprogramowanie klasy SIEM, w ograniczonym zakresie funkcjonalnym i ograniczonym zakresie monitorowanych systemów.

## Słownik pojęć

1. **Zdarzenie** – zestaw informacji opisujących za pomocą zdefiniowanego wcześniej zbioru parametrów wystąpienie pewnego faktu, przy czym jednym z parametrów opisu faktu jest czas jego wystąpienia lub rejestracji.
2. **Zdarzenie elementarne lub bazowe** – zdarzenie dotyczące pojedynczego faktu, który wystąpił w elemencie monitorowanym.
3. **Źródło zdarzeń** – obiekt, który generuje zdarzenia o jednolitej strukturze, zdefiniowanym dopuszczalnym zakresie wartości parametrów opisujących występowanie faktów i zapisywanych lub przesyłanych za pomocą jednego, zdefiniowanego sposobu.
4. **Kolekcja** – zbieranie źródłowych danych w postaci zdarzeń.
5. **Filtracja** – to odrzucenie danego zdarzenia z przetwarzania na dowolnym etapie przetwarzania przed analizą.
6. **Normalizacja** – przekształcanie zebranych zdarzeń do jednolitej postaci, tj. do postaci w której niezależnie od źródła pochodzenia zdarzenia jest ono opisywane za pomocą tego samego zbioru atrybutów.

7. **Agregacja** - eliminacja nadmiarowych i zduplikowanych zdarzeń, poprzez zastąpienie wielokrotnego wystąpienia tego samego zdarzenia lub podobnych zdarzeń jednym zdarzeniem.
8. **Kategoryzacja** - przypisanie zdarzeń z różnych źródeł do pewnych ogólnych kategorii opisujących typ zdarzenia, np. nieudane logowanie do kategorii „Uwierzytelnianie” i „Nieudane akcje” niezależnie od tego czy zdarzenie nieudanego logowania dotyczy systemu operacyjnego, bazy danych czy aplikacji.
9. **Priorytetyzacja** - nadawanie zdarzeniom priorytetów wg jednolitej skali i wg zadanego algorytmu.
10. **Analiza** - stwierdzenie czy występują pewne informacje, które mogą wskazywać na niepożądane zachowania w monitorowanych systemach; prowadzenie: korelacji (wykrywania znanych, uprzednio określonych sekwencji zdarzeń) i wykrywanie anomalii (badanie odchyłeń parametrów systemu od stanu bazowego).
11. **Wizualizacja** - graficzna reprezentacja przetworzonej informacji w pojedynczej konsoli (konsolach) czasu rzeczywistego.
12. **Raportowanie** – możliwość sporządzania raportów z danych historycznych
13. **Modelowanie środowiska monitorowanego** – możliwość przechowywania i przetwarzania informacji o zasobach teleinformatycznych podlegających monitorowaniu np. serwerach czy urządzeniach sieciowych, w szczególności poprzez możliwość nadawania zasobom atrybutów i korzystania z tych atrybutów podczas analizy.

### Zestawienie wymagań funkcjonalnych

Nr	Opis wymagania
1.	SMB pozwala na monitorowanie zdarzeń z systemów teleinformatycznych pod kątem bezpieczeństwa informacji
2.	SMB jest przystosowany do przetwarzania danych typowych dla systemów teleinformatycznych w tym: <ul style="list-style-type: none"> <li>▪ Adresów IPv4/v6 i MAC</li> <li>▪ Nazw DNS</li> <li>▪ Identyfikatorów protokołów sieciowych rodziny TCP/IP</li> <li>▪ Portów protokołów sieciowych</li> <li>▪ Nazw i identyfikatorów użytkowników</li> <li>▪ Nazw i identyfikatorów procesów</li> <li>▪ Parametrów protokołów warstwy aplikacji (np. użytych metod, komend, funkcji aplikacji itp.)</li> <li>▪ Znaczników czasu i daty w różnych formatach</li> <li>▪ Lokalizacji fizycznej komponentu</li> </ul>
3.	SMB posiada mechanizmy pozwalające na modelowanie środowisk monitorowanych.
4.	SMB posiada mechanizmy pozwalające na gromadzenie informacji dotyczących podatności w systemach teleinformatycznych i korelowanie tych informacji z

Nr	Opis wymagania
	bieżącymi zagrożeniami (zdarzeniami)
5.	SMB posiada mechanizmy pozwalające na gromadzenie informacji dotyczących znaczenia biznesowego monitorowanych systemów takich jak i ich rola, krytyczność, wymagania zgodnościowe, platforma technologiczna itp.
6.	SMB posiada gotowe rozwiązania informatyczne pozwalające na kolekcję zdarzeń bezpieczeństwa dla systemów teleinformatycznych objętych zakresem projektu.
7.	SMB posiada narzędzia pozwalające na kolekcję zdarzeń bezpieczeństwa dla niestandardowych systemów teleinformatycznych, np. zdarzeń z aplikacji specyficznych dla zamawiającego.
8.	SMB normalizuje wszystkie zdarzenia.
9.	Mechanizmy kolekcji SMB są aktualizowane na bieżąco wraz z pojawianiem się nowych wersji źródeł danych.
10.	SMB posiada mechanizmy kategoryzacji zdarzeń, pozwalający na abstrakcję od konkretnych identyfikatorów zdarzeń specyficznych dla źródła do ogólnych typów zdarzeń bezpieczeństwa (np. logowanie się użytkownika do systemu, zatrzymanie usługi itp.)
11.	SMB pozwala na zbieranie i przetwarzanie informacji nie zdarzeniowych (np. informacji o stanie systemu monitorowanego czy jego konfiguracji)
12.	SMB posiada mechanizm reguł korelacyjnych, tj. mechanizm który w czasie rzeczywistym jest w stanie wykrywać wystąpienie zdarzeń spełniających zdefiniowane wcześniej kryteria oraz sekwencji zdarzeń spełniających zdefiniowane wcześniej kryteria i powiązanych ze sobą poprzez relacje pomiędzy atrybutami poszczególnych zdarzeń.
13.	Mechanizm reguł korelacyjnych SMB jest w pełni parametryzowany w zakresie reguł logicznych i parametrów zdarzeń badanych przez reguły, przy czym parametryzowanie nie wymaga prowadzenia prac o charakterze programistycznym.
14.	Mechanizm reguł korelacyjnych SMB pozwala na definiowanie reguł korelacyjnych o oknie czasowym (odstęp pomiędzy wystąpieniem pierwszego i ostatniego zdarzenia w szukanej sekwencji) co najmniej 8 dni.
15.	SMB pozwala na dostęp on-line do zdarzeń bazowych i wyników działania mechanizmu korelacji przez co najmniej 90 dni.
16.	Mechanizm reguł korelacyjnych systemu pozwala na jednoczesną implementację co najmniej 200 reguł korelacyjnych działających równocześnie na zdarzeniach w czasie rzeczywistym.
17.	Mechanizm reguł korelacyjnych może być wykorzystywany do analizy danych napływających na bieżąco, jak i dla danych historycznych (tj. uprzednio zebranych i przechowywanych obecnie w systemie).
18.	Mechanizm reguł korelacyjnych pozwala na wykonywanie korelacji na wynikach korelacji (korelacja łańcuchowa).
19.	Mechanizmy korelacji zdarzeń SMB muszą pozwalać na budowanie reguł korelacyjnych wykorzystujących jako dane wejściowe zarówno zdarzenia bazowe jak i wyniki działania innych reguł korelacyjnych.
20.	SMB udostępnia mechanizm wykrywania anomalii tj. mechanizm, który wykrywa w czasie rzeczywistym odstępstwa od uprzednio zdefiniowanych, oczekiwanych parametrów zachowania systemu monitorowanego. Definiowanie parametrów oczekiwanych może być wykonywane przez użytkownika SMB lub automatycznie przez SMB, lecz w tym drugim przypadku musi istnieć możliwość korekty przez użytkownika.
21.	Mechanizm wykrywania anomalii systemu jest w pełni parametryzowany w zakresie definiowania monitorowanych parametrów i warunków detekcji anomalii, przy czym parametryzowanie nie wymaga prowadzenia prac o charakterze programistycznym.

Nr	Opis wymagania
22.	Mechanizm wykrywania anomalii udostępnia co najmniej następujące metody definiowania oczekiwanych wartości parametrów systemów monitorowanych: średnia ruchoma, odchylenie standardowe, współczynnik skośności rozkładu losowego (lub inną miarę pozwalającą na badanie symetryczności rozkładu losowego) – zarówno w odniesieniu do liczby zdarzeń jak i wartości atrybutów zdarzeń, pod warunkiem, że atrybuty te mają charakter liczbowy.
23.	Mechanizm wykrywania anomalii SMB pozwala na jednoczesne śledzenie wartości co najmniej 200 parametrów.
24.	SMB posiada mechanizm generowania raportów na żądanie oraz wg zadanego harmonogramu i ich automatycznego przekazywania do zdefiniowanych osób. Raportowanie musi funkcjonować w ten sam sposób odniesieniu do zdarzeń z systemów monitorowanych jak i działania samego systemu oraz obiektów w nim zdefiniowanych (np. raportowanie o liczbie aktualnie działających reguł korelacyjnych).
25.	SMB posiada mechanizm pozwalający na generowanie wybranych raportów za okres dłuższy niż okres przechowywania zdarzeń bazowych (określony w wymaganiu 15.).
26.	SMB pozwala na definiowanie praw użytkowników w odniesieniu do komponentów funkcjonalnych systemu i dowolnych podzbiorów zdarzeń.
27.	SMB stosuje mechanizm zarządzania użytkownikami w oparciu o role (ang. <i>role based authorization</i> )
28.	SMB posiada pojedynczy interfejs użytkownika (konsolę) pozwalającą na dostęp do wszystkich danych zgromadzonych w systemie oraz na zarządzanie konfiguracją wszystkich elementów systemu (tzw. scentralizowane zarządzanie).
29.	Interfejs użytkownika powinien umożliwiać analizy danych typu <i>drill down</i> tzn. powinien pozwalać w szybki sposób uzyskać widok danych (zdarzeń) parametryzowany na podstawie aktualnie wyświetlanych danych (np. wyświetlenie tylko zdarzeń pochodzących z adresu IP zawartego w aktualnie pokazywanym na konsoli systemu zdarzeniu).
30.	Pojedynczy element analityczny powinien mieć długoterminową wydajność co najmniej 4000 zdarzeń na sekundę.
31.	Architektura SMB musi pozwalać na odseparowanie fizyczne i logiczne komponentów kolekcjonujących zdarzenia (tzw. agentów) od komponentów analitycznych.
32.	SMB pozwala na ograniczenia pasma sieciowego wykorzystywanego do przesyłania danych pomiędzy agentem kolekcjonującym zdarzenia i częścią analityczną.
33.	SMB stosuje mechanizmy zapewniające integralność i poufność danych przy przesyłaniu danych pomiędzy agentem kolekcjonującym zdarzenia i częścią analityczną oraz przy przesyłaniu danych pomiędzy interfejsem użytkownika i częścią analityczną.
34.	SMB pozwala na jednoczesne korzystanie z systemu przez co najmniej 10 użytkowników.
35.	SMB może współpracować ze źródłami danych typu HP OpenView, IBM Tivoli.

## Zakres monitorowania

W ramach wdrożonego SMB monitorowaniem objęte zostaną następujące źródła zdarzeń:

Lista źródeł podlegających monitorowaniu:

1. Microsoft AD – 4 kontrolery Windows 2008 i 400 aktywnych użytkowników domenowych.
2. Serwer WWW – 1 szt. (system operacyjny freeBsd)

3. Microsoft ISA – 1 szt.
4. System bezpieczeństwa McAfee – 1 serwer na około 400 użytkowników
5. firewalle Cisco ASA wraz z modułami IPS – 2 klastry po 2 sztuki
6. firewalle Cisco FWSM – 2 klastry po 2 sztuki
7. routery internetowe Cisco 7200 – 2 sztuki
8. router internetowy Cisco XR 12404 – 1 sztuka
9. główne przełączniki rdzeniowe Catalyst – 4 sztuki
10. firewalle Cisco ASA w OW – 16 klastrów po 2 sztuki
11. urządzenia Cisco Ironport serii S (webowe) – 2 sztuki
12. serwery uwierzytelniające Cisco ACS – 2 sztuki
13. serwery uwierzytelniające RSA – 2 sztuki

Sumarycznie przewidywanych do podłączenia jest 60 źródeł danych (rozumianych jako serwer/urządzenie sieciowe), generujących średnio za okres 1 doby do 2500 zdarzeń na sekundę i o średniej objętości zdarzeń bazowych (logów) nie przekraczających 100 GB w ciągu doby.

Przewidywanych jest 2 użytkowników SMB, korzystających z funkcji przeglądania danych i korzystania z zaimplementowanych mechanizmów funkcjonalnych oraz 1 użytkownik SMB korzystający z funkcjonalności konfiguracji systemu, i zaawansowanych funkcji analitycznych.

### **Wymagania dla implementowanych mechanizmów funkcjonalnych**

W ramach projektu konieczne jest zaproponowanie, co najmniej 30 problemów bezpieczeństwa, które mogą być zaadresowane przez mechanizmy funkcjonalne SMB, w celu ich wykrywania i reakcji. W trakcie projektu, w wyniku uzgodnień pomiędzy zamawiającym a oferentem zostanie wybranych 5 problemów bezpieczeństwa, które zostaną zaimplementowane przez oferenta w SMB w ramach realizacji projektu. Przez problem bezpieczeństwa rozumiany jest zespół zdarzeń, których wystąpienie oznacza wystąpienie naruszenia bezpieczeństwa informacji zamawiającego lub możliwość wystąpienia takiego naruszenia w przyszłości – przykładami problemów mogą być: wielokrotne nieudane logowanie, wykonywanie operacji administracyjnych z konta użytkownika, który takich uprawnień nie powinien posiadać itp.

W ramach projektu konieczne jest także zamodelowanie, środowisk monitorowanych objętych zakresem wdrożenia oraz implementacja profili uprawnień co najmniej 3 ustalonych z zamawiającym ról użytkowników systemu.

### **Zakres prac**

Zakres projektu musi obejmować:

1. Zebranie informacji szczegółowych dotyczących monitorowanych źródeł i przygotowanie projektu technicznego SMB obejmującego swoim zakresem proponowaną architekturę techniczną, przepływy danych, projekt konfiguracji oprogramowania wchodzącego w skład SMB, projekt sposobu backupu SMB, projekt sposobu kolekcji zdarzeń z monitorowanych źródeł.
2. Dostarczenie licencji oprogramowania niezbędnego do uruchomienia SMB.
3. Instalację i uruchomienie SMB zgodnie z projektem technicznym, w tym podłączenie źródeł danych do systemu.
4. Zaproponowanie mechanizmów funkcjonalnych, które będą implementowane w SMB i uzgodnienie ich ostatecznego kształtu z zamawiającym.
5. Implementację uzgodnionych mechanizmów funkcjonalnych w SMB.

6. Opracowanie dokumentacji powykonawczej SMB, obejmującej opis konfiguracji sprzętowo-programową systemu, konfiguracji agentów, konfiguracji części analitycznej, konfiguracji zaimplementowanych mechanizmów funkcjonalnych.
7. Przeprowadzenie warsztatów szkoleniowych dla zespołu pracowników zamawiającego (5 osób), z obsługi i utrzymania SMB.

### **Wymagania sprzętowe**

Zamawiający wymaga aby proponowane rozwiązanie było zainstalowane na obecnie posiadanych serwerach. Zamawiający dopuszcza zastosowanie technologii wirtualizacyjnej.

Zamawiający posiada następujące serwery

4 serwery x86 typu Blade po dwa procesory 4 rdzeniowe Xeon, 32 GB RAM wraz z systemem operacyjnym Red Hat Linux 5 lub Windows 2008.

Macierz dyskowa EMC – około 1TB wolnej przestrzeni dyskowej

Specyficzne, elementy dodatkowe – jak stacje monitorujące wraz z zainstalowanym systemem operacyjnym oraz oprogramowaniem do zarządzania systemem monitoringu – Wykonawca ma umieścić w swojej ofercie.

Stacje monitorujące ( 5 szt.) powinny mieć następujące parametry:

- procesor Intel Core i7 Mobile o częstotliwości taktowania min. 2 GHz **brać równoważny**
- przekątna ekranu 12.1” WXGA+
- 4 GB RAM DDR3
- Dysk twardy w technologii SSD min. 120 GB
- Wewnętrzna karta WiFi wireless LAN, wewnętrzny moduł Bluetooth, wewnętrzny modem WWAN 3G z GPS bez SIMLOCK
- minimum 3 porty USB 2.0
- karta rozszerzeń 1 x Express Card 54/34
- Stacja dokująca wraz z nagrywką DVD DL
- waga wraz ze standardową baterią poniżej 1,5 kg
- dodatkowy zasilacz do stacji dokującej
- dodatkowa bateria o podwyższonej pojemności (9 Cell)

### **Zawartość oferty**

- 1) Wykaz charakterystyki funkcjonalnej oferowanego produktu w ujęciu całościowym oraz w rozbiciu na moduły funkcjonalne (zgodnie z załącznikiem nr 7),
- 2) Wykaz stacji monitorujących (zgodnie z załącznikiem nr 8),
- 3) Oświadczenie o poszczególnych cenach jednostkowych stacji monitorujących ( zgodnie z załącznikiem nr 9),
- 4) Oświadczenie o poszczególnych cenach jednostkowych licencji(zgodnie z załącznikiem nr 10).

**UMOWA ...../2010**

zawarta w dniu ..... 2010 r. w Warszawie pomiędzy Narodowym Funduszem Zdrowia Centralą z siedzibą w Warszawie przy ul. Grójeckiej 186, NIP 107-00-010-57, zwanym dalej ZAMAWIAJĄCYM, reprezentowanym przez:

a  
.....zwanym dalej WYKONAWCĄ, reprezentowaną przez:

W wyniku przeprowadzonego postępowania o udzielenie zamówienia w trybie przetargu nieograniczonego, zgodnie z przepisami ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity Dz. U. z 2010 Nr 113, poz. 759), została zawarta umowa następującej treści:

## § 1

1. Przedmiotem umowy jest „**Wdrożenie systemu monitorowania bezpieczeństwa w środowisku systemów informatycznych NFZ**” zgodnie z opisem technicznym i funkcjonalnym stanowiącym załącznik nr 1 do umowy.
2. **Przez wdrożenie systemu monitorowania bezpieczeństwa w NFZ Zamawiający rozumie dostawę licencji, dostawę urządzeń, zaprojektowanie systemu oraz jego uruchomienie, a także przeprowadzenie warsztatów.**

## § 2

1. Strony ustalają, że: zamówienie zostanie zrealizowane w terminie nie przekraczającym **20 tygodni** od dnia podpisania umowy.
2. Odbiór dostaw i prac potwierdzony zostanie protokołem odbioru, którego wzór stanowi załącznik nr 2, podpisanym przez przedstawicieli Stron, do którego załącznikami będą:
  - 1) dokumenty potwierdzające prawo do użytkowania oraz własność licencji,
  - 2) dokumenty potwierdzające gwarancje oraz okres i zakres usług serwisowych i konserwacyjnych
  - 3) komplet dokumentacji technicznej i funkcjonalnej,
  - 4) komplet instrukcji w języku polskim.
3. Niniejsza umowa obejmuje prawo do korzystania z licencji na następujących polach eksploatacji:
  - 1) wprowadzanie do pamięci komputerowej;
  - 2) użytkowanie zgodnie z dokumentacją i przeznaczeniem w szczególności w zakresie:
    - a) projektowanie, przygotowanie i adaptacja zastosowań Systemu zgodnie z potrzebami Zamawiającego,
    - b) dystrybucja zastosowań Systemu przez Zamawiającego oraz wymienianie we wszelkich materiałach informacyjnych lub promocyjnych,
    - c) zbieranie danych,
    - d) wprowadzanie danych,
    - e) utrwalanie danych,
    - f) przechowywanie danych,
    - g) opracowywanie danych,
    - h) zmienianie danych,
    - i) usuwanie danych,
    - j) odtwarzanie danych,
    - k) przesyłanie danych,
    - l) udostępnianie danych,
    - m) publikowanie danych w Internecie lub innych mediach,
  - 3) duplikowanie Systemu wynikające z potrzeby zabezpieczenia ciągłości jego użytkowania,
  - 4) odtwarzanie Systemu z kopii zapasowych
4. Protokół odbioru, o którym mowa w ust. 2 podpisany będzie ze strony Zamawiającego przez Naczelnika Wydziału Eksploatacji Departamentu Informatyki, lub upoważnionego do tego pracownika Departamentu Informatyki, po uprzednim parafowaniu go przez pracowników Departamentu Informatyki realizujących czynności techniczne i opiekę wdrożeniową. Ewentualne protokoły cząstkowe powinny stanowić odpowiednio ponumerowane załączniki.
5. Do realizacji czynności związanych z przedmiotem umowy ze strony Zamawiającego upoważnia się .....

6. W ramach niniejszej umowy Wykonawca przeprowadzi na rzecz Zamawiającego warsztaty z zakresu: instalacji, administracji, konfiguracji oraz strojenia (dostosowania systemu do bieżących potrzeb Centrali NFZ i Oddziałów Wojewódzkich NFZ) w następujących trybach:
  - 1) warsztaty w trakcie realizacji wdrożenia w wymiarze nie mniejszym niż 2 dni robocze
  - 2) warsztaty po zakończeniu wdrożenia w wymiarze nie mniejszym niż 5 dni roboczych
  - 3) zakres warsztatów: administracja, konfiguracja i strojenia (adaptacja do bieżących wymagań Centrali i Oddziałów Wojewódzkich NFZ),
  - 4) warsztaty zostaną przeprowadzone przez osoby posiadające kwalifikacje uprawniające do ich prowadzenia, potwierdzone certyfikatem,
  - 5) w ramach warsztatów Wykonawca zapewni odpowiednie materiały pomocnicze dla każdego uczestnika, adekwatne do zakresu szkolenia,
  - 6) Wykonawca wystawi uczestnikom zaświadczenia o odbytych warsztatach.
7. Do zadań Wykonawcy, w ramach realizacji umowy, należy w szczególności:
  - 1) pełny nadzór projektowy, czyli przygotowanie: założeń projektowych, harmonogramu, określenie warunków realizacji, oceny ryzyka,
  - 2) delegowanie odpowiedniej liczby specjalistów do realizacji projektu tak aby realizacja przebiegała bez zakłóceń i zakończyła się w terminie,
  - 3) przedkładanie na życzenie Zamawiającego raportów cząstkowych z realizacji kolejnych etapów projektu oraz raportu końcowego będącego podstawą do podpisania protokołu odbioru,
  - 4) realizacja dostaw oraz wdrożenia systemu według wymagań określonych przez Zamawiającego.

### § 3

1. Za wykonanie przedmiotu umowy Wykonawca otrzyma wynagrodzenie w łącznej wysokości ..... zł (słownie: ..... ) netto, powiększonej o należny podatek VAT, czyli wynagrodzenie brutto w wysokości ..... zł (słownie: .....).
2. Wykaz cen jednostkowych stanowi załącznik nr 3 do umowy.
3. Podstawą do wystawienia faktury za realizację przedmiotu umowy jest protokół odbioru, o którym mowa w § 2 ust. 2.
4. Zapłata wynagrodzenia nastąpi przelewem na rachunek bankowy WYKONAWCY w terminie 14 dni od dnia otrzymania przez Zamawiającego prawidłowo wystawionej faktury wraz z podpisanym przez przedstawicieli Stron protokołem odbioru przedmiotu umowy.
5. Za datę zapłaty Strony ustalają dzień, w którym Zamawiający wydał swojemu bankowi polecenie przelewu wynagrodzenia na konto Wykonawcy wskazane na fakturze.
6. Zamawiający zapłaci Wykonawcy za opóźnienie w zapłacie, odsetki ustawowe za okres od dnia wymagalności do dnia zapłaty.

### § 4

1. Po zakończeniu wdrożenia i odbiorze dostawy na podstawie protokołu odbioru, Wykonawca zobowiązuje się do zapewnienia gwarancji oraz wsparcia technicznego i konserwacyjnego dla oprogramowania według zasad opisanych w ustępach 2 do 9 niniejszego paragrafu.
2. *Gwarancja dla urządzeń (okres gwarancji liczony od daty podpisania protokołu odbioru):* Wykonawca na dostarczone, zamontowane i uruchomione stacje monitorujące udziela 12 miesięcznej gwarancji (gwarancja typu, ang.: „On-Site” **5/11**
3. Strony ustalają, że serwis gwarancyjny prowadzony będzie w miejscu wskazanym w zgłoszeniu awarii.
4. W przypadku uszkodzenia podzespołów zawierających lub będących nośnikami danych osobowych Zamawiający zastrzega sobie, aby diagnostyka awarii została przeprowadzona przez Wykonawcę w miejscu wskazanym w zgłoszeniu awarii, przy udziale pracowników Zamawiającego a wymiana elementów uszkodzonych na wolne od wad nie jest uwarunkowana koniecznością zwrotu Wykonawcy podzespołów podlegających wymianie.
5. Wszystkie koszty związane ze świadczeniem gwarancji ponosi Wykonawca.
6. Wykonawca zobowiązuje się do zapewnienia wsparcia technicznego i konserwacyjnego dla oprogramowania (okres wsparcia liczony od daty podpisania protokołu odbioru) na następujących zasadach:



- 1) w przypadku wystąpienia awarii lub dysfunkcyjności zaimplementowanego i eksploatowanego oprogramowania, Wykonawca będzie świadczyć wsparcie techniczne w trybie 7/24 z gwarantowanym czasem reakcji (zebranie niezbędnych danych do określenia przyczyny awarii i podjęcie działań naprawczych) 8 godzin oraz ze standardowym czasem naprawy nie dłuższym niż 48 godzin (całkowity czas usunięcia awarii nie dłuższy niż:  $8 + 48 = 56$  godzin),
  - 2) Wykonawca niezwłocznie usunie awarię lub dysfunkcyjność oprogramowania nie później niż w ciągu 56 godzin od momentu zgłoszenia.
  - 3) jeżeli usunięcia awarii lub dysfunkcyjności oprogramowania trwałaby dłużej niż 56 godzin od momentu zgłoszenia, Wykonawca na czas jej trwania dostarczy, po uzgodnieniu z Zamawiającym rozwiązanie zastępcze. Dłuższe niż 56 godzin usuwanie awarii lub dysfunkcyjności oprogramowania jest dopuszczalne po uprzedniej akceptacji Zamawiającego.
  - 4) całkowity czas usunięcia awarii lub dysfunkcyjności oprogramowania oraz przywrócenia pierwotnej sprawności operacyjnej i funkcjonalnej oprogramowania, w przypadku akceptacji przez Zamawiającego dłuższej niż 56 godzin naprawy, liczony od daty zgłoszenia awarii przez Zamawiającego nie może przekroczyć 28 dni kalendarzowych.
  - 5) w przypadku zapotrzebowania na modyfikację zaimplementowanego i eksploatowanego oprogramowania (zmiana funkcjonalności, rozbudowa, rekonfiguracja, modernizacja), świadczona będzie usługa wsparcia konserwacyjnego w trybie indywidualnego uzgodnienia przez Wykonawcę i Zamawiającego: wymagań, warunków realizacji, harmonogramu oraz powołania zespołu zadaniowego do realizacji zapotrzebowania Zamawiającego.
  - 6) Wykonawca w ramach ww. opisanego wsparcia przeprowadzi, na życzenie jednostki administracyjnej Zamawiającego, czyli Centrali lub Oddziału Wojewódzkiego, jednodniową analizę i strojenie oprogramowania. Zadanie to będzie wykonane w dowolnym - wybranym przez jednostkę administracyjną Zamawiającego i uzgodnionym z Wykonawcą – terminie.
7. Strony ustalają, że zgłaszanie awarii oprogramowania może nastąpić faksem albo za pomocą poczty elektronicznej (e-mail), w ciągu całej doby przez 7 dni w tygodniu w okresie świadczenia gwarancji oraz usługi wsparcia technicznego i konserwacyjnego opisanego w ust. 1 Zgłoszenie awarii Zamawiający będzie wysyłał za pomocą faksu na numer....., lub za pomocą poczty elektronicznej, adres: .....
8. Uzyskanie potwierdzenia przyjęcia faksu lub poczty elektronicznej z urządzeń technicznych udostępnionych lub wskazanych przez Wykonawcę, jako właściwych do zgłaszania awarii, traktowane będzie przez Zamawiającego, jako skuteczne zgłoszenie o awarii.
9. Wykonawca wykonuje naprawy na podstawie zgłoszenia awarii przez Zamawiającego, dokonanego zgodnie z formularzem, którego wzór stanowi załącznik nr 4 do umowy.

#### § 5

1. Wykonawca zobowiązuje się do działania na rzecz Zamawiającego zgodnie z przepisami ustawy o ochronie danych osobowych z 29 sierpnia 1997 r. (Dz. U. z 2002 r. Nr 101, poz.926, z późn. zm.). Za naruszenie przepisów w zakresie ochrony danych osobowych oraz ochrony informacji niejawnych przez oddelegowanych do świadczenia usługi pracowników, pełną odpowiedzialność ponosić będzie Wykonawca.
2. Wykonawca zobowiązany jest do podpisania przez pracowników Wykonawcy, oświadczenia stanowiącego załącznik nr 5 do umowy.
3. Umowa o zachowaniu poufności zostanie zawarta pomiędzy Stronami zgodnie z załącznikiem nr 6 do niniejszej umowy.
4. Wszelkie informacje uzyskane przez Wykonawcę w związku z realizacją niniejszej umowy podlegają ochronie i nie mogą być bez pisemnej zgody Zamawiającego przekazane innym podmiotom lub wykorzystane w innym celu niż realizacja treści niniejszej umowy.

#### § 6

1. Wykonawca wnosi zabezpieczenie należytego wykonania umowy w wysokości 10 % ceny brutto, o której mowa w § 3 ust. 1 tj. .... (słownie: .....złotych).
2. Jeżeli Wykonawca wykona dostawę i wdrożenie zgodnie z umową, zabezpieczenie zostanie zwolnione Wykonawcy w terminie 30 dni od dnia wykonania zamówienia i uznania przez Zamawiającego za należycie wykonane.

#### § 7

Zamawiający może odstąpić od umowy w terminie 7 dni od daty stwierdzenia nienależytego jej wykonania lub wykonania w sposób sprzeczny z ofertą.

#### § 8

1. Wykonawca zapłaci Zamawiającemu karę umowną:

- 1) za odstąpienie od umowy przez Zamawiającego z przyczyn, o których mowa w § 7 w wysokości 5 % wynagrodzenia brutto określonego w § 3 ust. 1,
  - 2) za opóźnienie w oddaniu przedmiotu umowy w wysokości 0,2 % wynagrodzenia brutto określonego w § 3 ust. 1 za każdy dzień opóźnienia,
  - 3) za opóźnienie terminu usunięcia awarii oprogramowania o którym mowa w § 4 ust. 6, pkt. 1. w wysokości 0,05 % wynagrodzenia brutto określonego w § 3 ust. 1 za każdą rozpoczętą godzinę opóźnienia,
  - 4) za niezrealizowanie z winy Wykonawcy warsztatów, o których mowa w § 2 ust. 6 w terminie uzgodnionym z Zamawiającym w wysokości 2 % wynagrodzenia brutto określonego w § 3 ust. 1.
2. Zamawiającemu przysługuje prawo dochodzenia odszkodowania przewyższającego wysokość zastrzeżonych kar umownych na zasadach ogólnych.
  3. Zamawiający zastrzega sobie prawo potrącenia naliczonej kary umownej, o której mowa w ust. 1 i odszkodowania z przysługującego Wykonawcy wynagrodzenia wynikającego z wystawionej faktury oraz zabezpieczenia należytego wykonania umowy na co Wykonawca wyraża zgodę.

#### § 9

1. Każda zmiana postanowień niniejszej umowy wymaga formy pisemnej, pod rygorem nieważności.
2. Strony wyrażą zgodę na zmianę wynagrodzenia Wykonawcy, o którym mowa w § 3 w przypadku zmiany stawek podatku od towarów i usług (VAT). Zmiana będzie polegać na doliczeniu do ceny netto wynikającej ze złożonej przez Wykonawcę oferty obowiązującego na dzień wystawienia faktury podatku VAT.

#### § 10

W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, Zamawiający może odstąpić od umowy. W takim wypadku WYKONAWCA może żądać jedynie wynagrodzenia należnego mu z tytułu wykonania części umowy.

#### § 11

Spory powstałe na tle realizacji niniejszej umowy będą rozstrzygane przez sąd właściwy miejscowo dla siedziby Zamawiającego.

#### § 12

W sprawach nie uregulowanych w umowie zastosowanie mają przepisy ustawy Prawo zamówień publicznych oraz przepisy Kodeksu cywilnego.

#### § 13

Umowę sporządzono w trzech jednobrzmiących egzemplarzach, dwa egzemplarze dla Zamawiającego, jeden dla Wykonawcy.

ZAMAWIAJĄCY

WYKONAWCA

**WZÓR PROTOKOŁU ODBIORU**

<b>Protokół odbioru</b> <b>Umowa ..... z dnia .....</b>	
<b>Narodowy Fundusz Zdrowia Odbierający</b>	
<b>Data odbioru</b>	

<b>Przedmiot odbioru</b>
<b>Wdrożenie systemu monitorowania bezpieczeństwa w środowisku systemów informatycznych NFZ</b> zgodnie z opisem technicznym i funkcjonalnym stanowiącym załącznik nr 1 do umowy ..... z dnia .....

Załączniki do Protokołu Odbioru:

1. dokumenty potwierdzające gwarancje na przekazany sprzęt
2. komplet dokumentacji technicznej dostarczonego systemu

**Podpis pracownika Departamentu Informatyki**

**Podpis Osoby Przekazującej**

**Podpis Osoby Odbierającej**

<b>ZGŁOSZENIE Nr / *</b>
<b>UZUPEŁNIENIE ZGŁOSZENIA Nr / *</b>

**Wypełnia Zgłaszający:**

Imię i Nazwisko:

Opis awarii :	Uwagi :
Data i godzina:	Podpis Zgłaszającego:

**Wypełnia Wykonawca :**

Przyjmujący zgłoszenie:	Uwagi:
Imię i Nazwisko przyjmującego:	
Data i godzina przyjęcia zgłoszenia:	

**Potwierdzenie realizacji zgłoszonej awarii:**

Data	Opis czynności	Czas	Uwagi
Data i podpis wykonawcy		Data i podpis Zgłaszającego awarie	

\*) Niepotrzebne skreślić

Pozostałe uwagi umieszczono na odwrocie karty

(imię i nazwisko)

(adres zamieszkania)

(nazwa i nr dokumentu tożsamości)

### OŚWIADCZENIE

***Oświadczam, że znana jest mi definicja danych osobowych w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r. Nr 101, poz. 926 z późn. zm.) w myśl, której za dane uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.***

**Zobowiązuję się:**

- 1) do zachowania w tajemnicy danych przetwarzanych przez Narodowy Fundusz Zdrowia wraz ze sposobami ich zabezpieczenia;
- 2) nie pozostawiać bez dozoru, ani udostępniać osobom nieupoważnionym dokumentów materialnych (w formie elektronicznej, papierowej itp.) z danymi;
- 3) nie wykorzystywać ani nie udostępniać nieuprawnionym dokumentacji z danymi do innych celów niż służbowe Narodowego Funduszu Zdrowia;
- 4) do niezwłocznego zniszczenia, w sposób uniemożliwiający zidentyfikowanie danych, wydrukowanych nadmiarowo, niepotrzebnych lub błędnych dokumentów;
- 5) w przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych, bezzwłocznie powiadomić Administratora Bezpieczeństwa Informacji Narodowego Funduszu Zdrowia, administratora systemu informatycznego, właściwego ze względu na zaistniały incydent kierownika komórki organizacyjnej w Narodowym Funduszu Zdrowia, a po godzinach urzędowania również ochronę obiektu;
- 6) przy przetwarzaniu danych, do szczególnej dbałości o zachowanie poufności, integralności i dostępności danych związanych z dokumentami znajdującymi się w obrocie w Narodowym Funduszu Zdrowia, także dotyczących danych pracowników, dokumentacji systemu przetwarzania danych oraz infrastruktury sprzętowo - programowej systemów informatycznych;
- 7) przy przetwarzaniu danych poza systemem informatycznym, do szczególnej dbałości o zachowanie poufności treści dokumentów, które znajdują się w obrocie w Narodowym Funduszu Zdrowia, oraz przestrzegania zasad dostępu do danych.

Wykonano w 2 jednobrzmiących egzemplarzach

Potwierdzam odbiór 1 egzemplarza

.....  
Miejscowość, data

.....  
czytelny podpis

**UMOWA O ZACHOWANIU POUFNOŚCI**

zawarta dnia .....2010 roku w Warszawie (dalej „Umowa”), pomiędzy:

.....

a

**Narodowym Funduszem Zdrowia** z siedzibą w Warszawie (02-390), przy ulicy Grójeckiej 186.....

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

zwanych dalej łącznie „Stronami”

ZWAŻYWSZY, Na zawarcie umowy między Stronami na „**Wdrożenie systemu monitorowania bezpieczeństwa w środowisku systemów informatycznych NFZ**” umowa nr ...../2010

NINIEJSZYM POSTANAWIA SIĘ, CO NASTĘPUJE:

**1. Wykładnia**

1.1 W niniejszej Umowie następujące słowa i wyrażenia uważa się, tam, gdzie pozwala na to kontekst, za użyte w następujących znaczeniach:  
 „Informacje Poufne” oznaczają:

(a) wszelkie informacje lub dane, ustne, na piśmie lub zapisane w inny sposób, dotyczące spraw, planów działalności gospodarczej lub przedsięwzięć Strony, przekazywane drugiej stronie, oraz

(b) wszelkie rozmowy lub rokowania prowadzone pomiędzy przedstawicielami stron oraz przekazywane w ich trakcie informacje,

(c) wszelkie informacje, rozmowy i rokowania, prowadzone ze stroną trzecią zaangażowaną W proces współpracy na wniosek dowolnej ze stron.

**2. Zobowiązania**

2.1 Z uwagi na wzajemne udostępnianie sobie Informacji Poufnych każda ze stron zobowiązuje się:

(a) zachować w tajemnicy wszystkie Informacje Poufne drugiej Strony, niezależnie od formy ich przekazania;

(b) wykorzystywać lub stosować Informacje Poufne drugiej Strony wyłącznie na użytek współpracy oraz tak, aby ustalić, czy i na jakich warunkach Strony mogłyby pragnąć przystąpić do działań;

(c) nie wykorzystywać, kopiować., adaptować, zmieniać, ujawniać, rezygnować

z posiadania, ani nie stosować Informacji Poufnych drugiej Strony bez zgody Strony, której to te Informacje Poufne dotyczą;

(d) w dowolnym czasie, bez względu na postać rokowań, nie kopiować, ujawniać lub udostępniać w inny sposób bez zgody drugiej Strony na piśmie, żadnych Informacji Poufnych drugiej Strony stronom trzecim innym niż:

(i) ci z jej członków zarządu lub pracowników, którzy muszą otrzymać i zapoznać się z Informacjami Poufnymi w związku ze współpracą, z zastrzeżeniem, że strona otrzymująca wyrazi pisemną zgodę na to, by wszyscy jej członkowie zarządu, członkowie kadry kierowniczej i pracownicy zostali poinformowani o postanowieniach niniejszego zobowiązania i wyrazili na nie pisemną zgodę; oraz

(ii) jej doradcy, z zastrzeżeniem, że strona otrzymująca wyrazi zgodę na to, by doradcy ci oraz ich pracownicy zostali poinformowani o postanowieniach niniejszego zobowiązania i wyrazili na nie pisemną zgodę;

(e) zapewnić odpowiedni i bezpieczny sposób przechowywania wszystkich Informacji Poufnych otrzymanych w formie materialnej w czasie, gdy znajdują się one na jej przechowaniu lub pod jego kontrolą; oraz

(f) na pisemny wniosek drugiej Strony lub w przypadku rozwiązania lub wygaśnięcia Umowy, niezwłocznie zwrócić lub zniszczyć na własny koszt wszelkie materiały zawierające jakiegokolwiek Informacje Poufne drugiej Strony wraz ze wszystkim kopiami, będącymi w jej posiadaniu lub w posiadaniu jej członków zarządu, członków kadry kierowniczej, pracowników i doradców.

2.2 W przypadku naruszenia przez jedną ze Stron obowiązków dotyczących Informacji Poufnych, o których mowa w niniejszej Umowie oraz zakazu konkurencji, o którym mowa w pkt. 2.3 i 2.4 poniżej, druga Strona uprawniona jest z tytułu poniesionej szkody do dochodzenia roszczeń odszkodowawczych na zasadach ogólnych, z wyłączeniem utraconych korzyści.

2.3 Strony Umowy zobowiązują się w trakcie prowadzenia rozmów do niepodjęcia współpracy z podmiotami konkurencyjnymi wobec którejkolwiek ze Stron Umowy w zakresie przedmiotu ewentualnej przyszłej współpracy pomiędzy Stronami.

2.4 Przez podmiot konkurencyjny w rozumieniu niniejszej Umowy rozumie się podmiot prowadzący wszelką działalność identyczną lub podobną, w całości lub w części, do działalności prowadzonej przez którąkolwiek ze Stron Umowy.

2.5 Ewentualni Podwykonawcy niniejszej umowy zobowiązani są przez Wykonawcę do przestrzegania zobowiązań wynikających z niniejszej umowy.

2.6 Pracownik Wykonawcy lub pracownik podwykonawcy, realizujący zadania na rzecz NFZ winien podpisać oświadczenie będące załącznikiem nr. 1 oraz dostarczyć je do koordynatora danych prac, ze strony zamawiającego.

### **3. Ograniczenia**

3.1 Zobowiązania określone w paragrafie 2 powyżej nie mają zastosowania do Informacji Poufnych:

(a) które są w dniu ujawnienia publicznie znane lub stają się następnie publicznie znane w dowolny sposób bez naruszenia niniejszej Umowy; lub

- (b) w odniesieniu do których Strona otrzymująca wykaże, że była w ich posiadaniu lub że były jej znane w związku z ich wykorzystywaniem, istnieniem w jej aktach, zapisach komputerowych lub na innych nośnikach zapisu przed ich otrzymaniem od Strony udostępniającej, lub które zostały opracowane dla Strony otrzymującej lub przez nią samą niezależnie od udostępnionych jej przez stronę udostępniającą Informacji Poufnych;
- (c) które zostaną udostępnione w sposób legalny stronie otrzymującej przez dowolną stronę trzecią i które nie stanowią przedmiotu żadnego ograniczenia w odniesieniu do ich wykorzystania lub ujawnienia, nałożonego na stronę trzecią lub przez nią samą w czasie niniejszego postanowienia; lub
- (d) których ujawnienie wymagane jest od Strony otrzymującej na mocy przepisów prawa.

3.2 Jeżeli Strona niniejszej Umowy zostanie zobowiązana na mocy prawa lub wezwania sądu do ujawnienia jakichkolwiek Informacji Poufnych, stanowiących własność drugiej Strony (Właściciela Informacji Poufnych), Strona ta, niezwłocznie zawiadomi na piśmie drugą Stronę niniejszej Umowy przed dokonaniem jakiegokolwiek ujawnienia.

3.3 Strona zobowiązana na mocy prawa lub wezwania sądu do ujawnienia Informacji Poufnych będzie uprawniona do ujawnienia tylko takiej części informacji Poufnej, jaka wymagana jest przez prawo, oraz zobowiązana do podjęcia wszelkich uzasadnionych środków, mających na celu upewnienie się, że Informacje Poufne są traktowane jako poufne.

#### **4. Prawa i gwarancje dotyczące Informacji Poufnych i wzajemnych negocjacji**

4.1 Każda ze Stron potwierdza i wyraża zgodę na to, że nie będzie uprawniona do nabycia w sposób dorozumiany lub inaczej żadnych praw do Informacji Poufnych przekazanych przez drugą Stronę lub od niej uzyskanych.

4.2 Żadna ze stron nie składa żadnych wyraźnych lub dorozumianych oświadczeń i zapewnień, co do kompletności Informacji Poufnych.

#### **5. Okres obowiązywania**

Niniejsza Umowa obowiązywać będzie przez okres 3 (trzech) lat od daty jej zawarcia. Bez względu na powyższe, zobowiązanie do zachowania tajemnicy i poufności pozostaje w mocy przez okres kolejnych 3 (trzech) lat od daty ostatniego udostępnienia Informacji Poufnych.

#### **6. Prawo właściwe**

6.1 Wszelkie spory wynikające z niniejszej Umowy powinny być rozstrzygane w drodze wzajemnego porozumienia Stron. Jeśli po upływie jednego miesiąca wzajemne porozumienie nie zostanie osiągnięte, właściwym do rozstrzygania sporu będzie sąd właściwy dla siedziby Narodowego Funduszu Zdrowia.

6.2 Do wszystkich kwestii nieuregulowanych w niniejszej Umowie znajdują zastosowanie szczególności przepisy kodeksu cywilnego oraz inne obowiązujące przepisy prawne.

#### **7. Egzemplarze Umowy**

Niniejsza Umowa sporządzona została w dwóch jednobrzmiących egzemplarzach po jednym egzemplarzu dla każdej ze Stron.



## 8. Zmiany do Umowy

Wszelkie zmiany postanowień niniejszej Umowy wymagają dla swej ważności zgody Stron, z zachowaniem formy pisemnej w postaci Aneksu pod rygorem nieważności.

Strony zawierają niniejszą Umowę za pośrednictwem należycie umocowanych przedstawicieli w dacie podpisania niniejszej Umowy.

Podpisano w imieniu:

.....

Podpisano w imieniu  
Narodowy Fundusz Zdrowia

.....

pieczęć Wykonawcy

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

**Oferta**

Nazwa Wykonawcy .....

Adres Wykonawcy .....

tel. .... fax .....

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

**składa ofertę na :****Wdrożenie systemu monitorowania bezpieczeństwa w środowisku systemów informatycznych NFZ****1. Oświadczenie o oferowanej cenie:**

- 1) cena netto ..... zł  
(słownie:.....)
- 2) podatek od towarów i usług VAT – ..... zł  
(słownie: .....) )
- 3) cena brutto ..... zł  
(słownie:.....)

**2. Oświadczenie o akceptacji terminu realizacji zamówienia:**

Oświadczam, że bez zastrzeżeń przyjmuję przedstawiony przez Zamawiającego termin realizacji zamówienia nie przekraczający 20 tygodni od daty podpisania umowy.

**3. Oświadczenie o akceptacji wymagań określających przedmiot zamówienia:**

Oświadczam, że akceptuję wszystkie wymagania określone w załączniku do Specyfikacji „Opis przedmiotu zamówienia” i stwierdzam, że **oferowany produkt** spełnia określone w nim wymogi w pełnym zakresie.

**4. Oświadczenie o akceptacji warunków płatności:**

Oświadczam, że bez zastrzeżeń przyjmuję przedstawione przez Zamawiającego warunki płatności za realizację zamówienia.

**5. Oświadczenie o akceptacji okresu gwarancji i wsparcia technicznego**

Oświadczam, że na bez zastrzeżeń przyjmuję przedstawione przez Zamawiającego warunki świadczenia gwarancji oraz wsparcia technicznego.

**6. Oświadczenie o akceptacji zasad zgłaszania awarii oraz terminów usuwania awarii**

Oświadczam, że na bez zastrzeżeń przyjmuję przedstawione przez Zamawiającego warunki zgłaszania oraz usuwania awarii.

.....  
**Podpis i pieczęć Wykonawcy**

**8. Oświadczenie o akceptacji przedstawionych przez Zamawiającego warunków umownych realizacji zamówienia:**

Oświadczam, że bez zastrzeżeń przyjmuję przedstawione przez Zamawiającego warunki umowne realizacji zamówienia określone we wzorze umowy załączonym do specyfikacji. Zobowiązuję się w przypadku wyboru naszej oferty do zawarcia umowy na wymienionych warunkach w miejscu i terminie wyznaczonym przez Zamawiającego.

**9. Oświadczenie Wykonawcy, czy wykona sam zamówienie, czy powierzy wykonanie części zamówienia podwykonawcom**

Oświadczamy, że realizację przedmiotu zamówienia:

wykonamy sami \*

powierzmy wykonanie części zamówienia podwykonawcom zgodnie z poniższym zestawieniem \*  
\* właściwe zaznaczyć

Lp.	Części zamówienia, których wykonanie Wykonawca powierzy podwykonawcom

**Ponadto:**

1. Uważamy się za związanych niniejszą ofertą przez czas wskazany w specyfikacji istotnych warunków zamówienia, czyli przez okres ..... dni od daty składania ofert.
2. Oświadczamy, że sposób reprezentowania Spółki lub wykonawców składających ofertę wspólną dla potrzeb niniejszego zamówienia jest następujący:  
.....  
(wypełniają jedynie wykonawcy prowadzący działalność w formie spółki lub składający ofertę wspólną)
3. Oświadczamy, iż – za wyjątkiem informacji i dokumentów zawartych w ofercie na stronach nr ..... - niniejsza oferta oraz wszelkie załączniki do niej są jawne i nie zawierają informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

**Oświadczenie o dokumentach załączonych do oferty:**

- 1) Wykaz charakterystyki funkcjonalnej oferowanego produktu w ujęciu całościowym oraz w rozbiciu na moduły funkcjonalne (zgodnie z załącznikiem nr 7),
- 2) Wykaz stacji monitorujących niezbędnych do wdrożenia oferowanego produktu (zgodnie z załącznikiem nr 8),
- 3) Oświadczenie o poszczególnych cenach jednostkowych stacji monitorujących (zgodnie z załącznikiem nr 9),
- 4) Oświadczenie o poszczególnych cenach jednostkowych licencji (zgodnie z załącznikiem nr 10),

.....  
**Podpis i pieczęć Wykonawcy**

pieczęć Wykonawcy

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

**OŚWIADCZENIE WYKONAWCY O SPEŁNIANIU WARUNKÓW UDZIAŁU  
W POSTĘPOWANIU**

.....  
.....  
/nazwa (firma) i adres Wykonawcy/

( w przypadku Wykonawców występujących wspólnie należy wymienić wszystkich Wykonawców )

Stosownie do treści art. 44 w zw. z art. 22 ust. 1 pkt 1-4 ustawy z dnia 29 stycznia 2004 r.  
Prawo zamówień publicznych (tj jednolity Dz. U. z 2010 Nr 113, poz. 759):

niniejszym oświadczam, że spełniamy warunki udziału w postępowaniu o zamówienie publiczne na:

**„Wdrożenie systemu monitorowania bezpieczeństwa w środowisku systemów informatycznych NFZ”**  
dotyczące:

- 1) posiadania uprawnień do wykonania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania,
- 2) posiadania wiedzy i doświadczenia,
- 3) dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonywania zamówienia,
- 4) sytuacji ekonomicznej i finansowej.

.....  
**podpis i pieczęć Wykonawcy\***

\* - w przypadku Wykonawców występujących wspólnie podpisuje Pełnomocnik lub wszyscy Wykonawcy

pieczęć Wykonawcy

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

**OŚWIADCZENIE WYKONAWCY O BRAKU PODSTAW DO WYKLUCZENIA**

.....

.....

/nazwa (firma) i adres Wykonawcy/

Oświadczam, że brak jest podstaw do wykluczenia nas z postępowania o udzielenie zamówienia w okolicznościach, o których mowa w art. 24 ust. 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (jednolity Dz. U. z 2010 Nr 113, poz. 759) w postępowaniu o zamówienie publiczne na:

**„Wdrożenie systemu monitorowania bezpieczeństwa w środowisku systemów informatycznych NFZ”**

.....

**podpis i pieczęć Wykonawcy\***

\* - w przypadku Wykonawców występujących wspólnie oświadczenie składa każdy Wykonawca

pieczęć Wykonawcy

**WYKAZ WYKONANYCH DOSTAW**

Wykaz wykonanych (a w przypadku świadczeń okresowych lub ciągłych uwzględniane są również wykonywane) w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, co najmniej 3 dostaw polegających **na wdrożeniu systemu monitorowania bezpieczeństwa w środowisku systemów informatycznych** **każda o wartości przekraczającej 200.000,00 zł brutto** z podaniem ich wartości, przedmiotu, dat wykonania i odbiorców oraz załączenia dokumentów potwierdzających, że dostawy te zostały wykonane lub są wykonywane należycie

Wykaz musi zawierać informacje niezbędne do stwierdzenia, czy Wykonawca spełnia warunek określony w punkcie 5.2 Specyfikacji. Do każdej wykonanej usługi (wskazanej w wykazie) należy przedstawić dokument potwierdzający, że usługa ta została wykonana należycie.

Datę wykonania zamówienia należy określić jako miesiąc i rok.

Przedmiot	Wartość zamówienia /brutto/ w PLN	Data wykonania /dzień, miesiąc i rok/	Nazwa i adres odbiorcy
1	2	3	4

Uwaga ! Wszystkie wartości należy podać w PLN.

**Wykonawcy zobowiązani są załączyć do oferty dokumenty potwierdzające, że wskazane w wykazie usługi zostały wykonane należycie.**

.....  
Podpis i pieczęć Wykonawcy

Nazwa Wykonawcy:

.....

Adres Wykonawca:

.....

**WYKAZ CHARAKTERYSTYKI FUNKCJONALNEJ OFEROWANEGO PRODUKTU  
W UJĘCIU CAŁOŚCIOWYM ORAZ W ROZBICIU NA MODUŁY FUNKCJONALNE.****Nazwa handlowa oferowanego oprogramowania**

.....

	<b>Opis cech wymaganych przez Zamawiającego</b>	<b>Opis cech produktu oferowanego przez Wykonawcę</b>	<b>Nazwa handlowa oferowanego produktu/modułu(ów)</b>	<b>Ilość licencji produktu/modułu</b>
1	Monitorowanie zdarzeń z systemów teleinformatycznych pod kątem bezpieczeństwa informacji			
2	Przystosowanie do przetwarzania danych typowych dla systemów teleinformatycznych w tym: <ul style="list-style-type: none"> <li>▪ Adresów IPv4 i MAC</li> <li>▪ Nazw DNS</li> <li>▪ Identyfikatorów protokołów sieciowych rodziny TCP/IP</li> <li>▪ Portów protokołów sieciowych</li> <li>▪ Nazw i identyfikatorów użytkowników</li> <li>▪ Nazw i identyfikatorów procesów</li> <li>▪ Parametrów protokołów warstwy aplikacji (np. użytych metod, komend, funkcji aplikacji itp.)</li> <li>▪ Znaczników czasu i daty w różnych formatach</li> <li>▪ Lokalizacji fizycznej komponentu</li> </ul>			
3	Mechanizm pozwalający na modelowanie środowisk monitorowanych.			
4	Mechanizm pozwalający na gromadzenie informacji dotyczących podatności w systemach teleinformatycznych i korelowanie tych informacji z bieżącymi zagrożeniami (zdarzeniami)			
5	Mechanizm pozwalający na gromadzenie informacji dotyczących znaczenia biznesowego monitorowanych systemów takich jak i ich rola, krytyczność, wymagania zgodnościowe, platforma			

	<b>Opis cech wymaganych przez Zamawiającego</b>	<b>Opis cech produktu oferowanego przez Wykonawcę</b>	<b>Nazwa handlowa oferowanego produktu/modułu(ów)</b>	<b>Ilość licencji produktu/modułu</b>
	technologiczna itp.			
6	Kolekcja zdarzeń bezpieczeństwa dla systemów teleinformatycznych objętych zakresem projektu.			
7	Kolekcja zdarzeń bezpieczeństwa dla niestandardowych systemów teleinformatycznych, np. zdarzeń z aplikacji specyficznych dla zamawiającego.			
8	Normalizacja wszystkich zdarzeń.			
9	Mechanizm aktualizowania na bieżąco wraz z pojawianiem się nowych wersji źródeł danych.			
10	Kategoryzacji zdarzeń, pozwalająca na abstrakcję od konkretnych identyfikatorów zdarzeń specyficznych dla źródła do ogólnych typów zdarzeń bezpieczeństwa (np. logowanie się użytkownika do systemu, zatrzymanie usługi itp.)			
11	Zbieranie i przetwarzanie informacji nie zdarzeniowych (np. informacji o stanie systemu monitorowanego czy jego konfiguracji)			
12	Mechanizm reguł korelacyjnych, tj. mechanizm który w czasie rzeczywistym jest w stanie wykrywać wystąpienie zdarzeń spełniających zdefiniowane wcześniej kryteria oraz sekwencji zdarzeń spełniających zdefiniowane wcześniej kryteria i powiązanych ze sobą poprzez relacje pomiędzy atrybutami poszczególnych zdarzeń.			
13	Mechanizm reguł korelacyjnych jest w pełni parametryzowany w zakresie reguł logicznych i parametrów zdarzeń badanych przez reguły, przy czym parametryzowanie nie wymaga prowadzenia prac o charakterze programistycznym.			
14	Mechanizm reguł korelacyjnych pozwala na definiowanie reguł korelacyjnych o oknie czasowym (odstęp pomiędzy wystąpieniem pierwszego i ostatniego zdarzenia w szukanej sekwencji) co najmniej 8 dni.			



	<b>Opis cech wymaganych przez Zamawiającego</b>	<b>Opis cech produktu oferowanego przez Wykonawcę</b>	<b>Nazwa handlowa oferowanego produktu/modułu(ów)</b>	<b>Ilość licencji produktu/modułu</b>
15	Dostęp on-line do zdarzeń bazowych i wyników działania mechanizmu korelacji przez co najmniej 90 dni.			
16	Mechanizm reguł korelacyjnych systemu pozwala na jednoczesną implementację co najmniej 200 reguł korelacyjnych działających równocześnie na zdarzeniach w czasie rzeczywistym.			
16	Mechanizm reguł korelacyjnych może być wykorzystywany do analizy danych napływających na bieżąco, jak i dla danych historycznych (tj. uprzednio zebranych i przechowywanych obecnie w systemie).			
18	Mechanizm reguł korelacyjnych pozwala na wykonywanie korelacji na wynikach korelacji (korelacja łańcuchowa).			
19	Mechanizmy korelacji zdarzeń SMB muszą pozwalać na budowanie reguł korelacyjnych wykorzystujących jako dane wejściowe zarówno zdarzenia bazowe jak i wyniki działania innych reguł korelacyjnych.			
20	Mechanizm wykrywania anomalii tj. mechanizm, który wykrywa w czasie rzeczywistym odstępstwa od uprzednio zdefiniowanych, oczekiwanych parametrów zachowania systemu monitorowanego. Definiowanie parametrów oczekiwanych może być wykonywane przez użytkownika			
21	Mechanizm wykrywania anomalii systemu jest w pełni parametryzowany w zakresie definiowania monitorowanych parametrów i warunków detekcji anomalii, przy czym parametryzowanie nie wymaga prowadzenia prac o charakterze programistycznym.			
22	Mechanizm wykrywania anomalii udostępnia co najmniej następujące metody definiowania oczekiwanych wartości parametrów systemów monitorowanych: średnia ruchoma, odchylenie standardowe, współczynnik skośności rozkładu losowego (lub inną miarę pozwalającą na badanie			

	Opis cech wymaganych przez Zamawiającego	Opis cech produktu oferowanego przez Wykonawcę	Nazwa handlowa oferowanego produktu/modułu(ów)	Ilość licencji produktu/modułu
	symetryczności rozkładu losowego) – zarówno w odniesieniu do liczby zdarzeń jak i wartości atrybutów zdarzeń, pod warunkiem, że atrybuty te mają charakter liczbowy.			
23	Mechanizm wykrywania anomalii pozwalający na jednoczesne śledzenie wartości co najmniej 200 parametrów.			
24	Mechanizm generowania raportów na żądanie oraz wg zadanego harmonogramu i ich automatycznego przekazywania do zdefiniowanych osób. Raportowanie musi funkcjonować w ten sam sposób odniesieniu do zdarzeń z systemów monitorowanych jak i działania samego systemu oraz obiektów w nim zdefiniowanych (np. raportowanie o liczbie aktualnie działających reguł korelacyjnych).			
25	Mechanizm pozwalający na generowanie wybranych raportów za okres dłuższy niż okres przechowywania zdarzeń bazowych (określony w wymaganiu 15.).			
26	Definiowanie praw użytkowników w odniesieniu do komponentów funkcjonalnych systemu i dowolnych podzbiorów zdarzeń.			
27	Mechanizm zarządzania użytkownikami w oparciu o role (ang. <i>role based authorization</i> )			
28	Pojedynczy interfejs użytkownika (konsola) pozwalający na dostęp do wszystkich danych zgromadzonych w systemie oraz na zarządzanie konfiguracją wszystkich elementów systemu (tzw. scentralizowane zarządzanie).			
29	Interfejs użytkownika - umożliwienie analizy danych typu <i>drill down</i> tzn. powinien pozwalać w szybki sposób uzyskać widok danych (zdarzeń) parametryzowany na podstawie aktualnie wyświetlanych danych (np. wyświetlenie tylko zdarzeń pochodzących z adresu IP zawartego w aktualnie pokazywanym na konsoli systemu zdarzeniu).			

	<b>Opis cech wymaganych przez Zamawiającego</b>	<b>Opis cech produktu oferowanego przez Wykonawcę</b>	<b>Nazwa handlowa oferowanego produktu/modułu(ów)</b>	<b>Ilość licencji produktu/modułu</b>
30	Pojedynczy element analityczny powinien mieć długoterminową wydajność co najmniej 4000 zdarzeń na sekundę.			
31	Architektura musi pozwalać na odseparowanie fizyczne i logiczne komponentów kolekcjonujących zdarzenia (tzw. agentów) od komponentów analitycznych.			
32	Możliwość ograniczenia pasma sieciowego wykorzystywanego do przesyłania danych pomiędzy agentem kolekcjonującym zdarzenia i częścią analityczną.			
33	Mechanizm zapewniający integralność i poufność danych przy przesyłaniu danych pomiędzy agentem kolekcjonującym zdarzenia i częścią analityczną oraz przy przesyłaniu danych pomiędzy interfejsem użytkownika i częścią analityczną.			
34	Możliwość jednoczesnego korzystania z systemu przez co najmniej 10 użytkowników.			
35	Współpracowa ze źródłami danych typu HP OpenView, IBM Tivoli			

**Wykonawca jest zobowiązany do wypełnienia kolumny „Opis cech produktu oferowanego przez Dostawcę” odnosząc się do każdego szczegółowego opisu wymagania oraz szczegółowego opisu cech funkcji. Jeśli dana funkcja wymaga zastosowania kilku modułów w kolumnie „Nazwa oferowanego modułu/ów” należy podać wszystkie moduły składające się na daną funkcjonalność. W przypadku wpisania w kolumnie większej ilości modułów składających się na daną funkcjonalność w kolumnie „Ilość licencji” należy podać osobno ilość licencji na każdy moduł.**

.....  
 podpis i pieczęć Wykonawcy

Nazwa Wykonawcy:

.....

Adres Wykonawcy:

.....

**WYKAZ STACJI MONITORUJĄCYCH NIEZBĘDNYCH DO WDROŻENIA  
OFEROWANEGO PRODUKTU**

<b>Lp.</b>	<b>Nazwa handlowa urządzenia</b>	<b>Typ/rodzaj urządzenia</b>	<b>Przeznaczenie urządzenia</b>	<b>Ilość</b>

.....

podpis i pieczęć Wykonawcy

ZAŁĄCZNIK NR 9 DO SPECYFIKACJI  
Po zawarciu umowy stanowić będzie załącznik nr 3 do umowy

Nazwa Wykonawcy:

.....

Adres Wykonawcy:

.....

**OŚWIADCZENIE O POSZCZEGÓLNYCH CENACH JEDNOSTKOWYCH\* STACJI  
MONITORUJĄCYCH**

Lp.	Oznaczenie sprzętu	Cena jednostkowa netto (zł)	Niezbędna i dostarczona ilość (szt.)	Cena łączna netto (zł)	Podatek VAT (zł)	Cena łączna brutto (zł)
1						
2						
			<b>RAZEM</b>			

\* podane ceny powinny obejmować wartość dostawy urządzeń i instalacji.

.....

podpis i pieczęć Wykonawcy

Po zawarciu umowy stanowić będzie załącznik nr 3 do umowy

Nazwa Wykonawcy:

.....

Adres Wykonawcy:

.....

**OŚWIADCZENIE O POSZCZEGÓLNYCH CENACH JEDNOSTKOWYCH\* OFEROWANYCH LICENCJI**

Lp.	Nazwa licencji dla oprogramowania	Cena jednostkowa netto (zł)	Niezbędna i dostarczona ilość licencji	Wartość netto (zł)	Podatek VAT (zł)	Wartość brutto (zł)
1.	2.	3.	4.	5.	6.	7.
1.						
2.						
3.						
4.						
5.						
			<b>RAZEM</b>			

\* podane ceny powinny obejmować wartość licencji wraz z wdrożeniem.

.....  
podpis i pieczęć Wykonawcy