Kędzierzyn-Koźle, dn. 06.09.2024r.

ZAPYTANIE OFERTOWE NR AE/2/2024

1. ZAMAWIAJĄCY

Wojewódzki Ośrodek Medycyny Pracy w Opolu
z/s w Kędzierzynie-Koźlu
ul. Mikołaja Reja 2A, 47-220 Kędzierzyn-Koźle
REGON: 000637921
NIP: 749-15-51-479

2. TRYB UDZIELENIA ZAMÓWIENIA

Postępowanie o udzielenie niniejszego zamówienia prowadzone jest na podstawie Regulaminu udzielania zamówień publicznych o wartości do 130 000 zł w Wojewódzkim Ośrodku Medycyny Pracy w Opolu, z dnia 28.08.2023 r. znajdującego zastosowanie w przypadkach, dla których na podstawie art. 2 ust 1. pkt. 1 ustawy z dnia 11 września 2019 roku Prawo zamówień publicznych przepisów ww. ustawy nie stosuje się.

3. PRZEDMIOT ZAMÓWIENIA – OBEJMUJE 2 ZADANIA

3.1. ZADANIE I - OPIS

Dostarczenie, instalacja i wdrożenie systemów z dziedziny cyberbezpieczeństwa w postaci urządzeń **UTM STORMSHIELD** dla trzech lokalizacji tj.

1 Minimum SN320 Premium Security Pack + Next Business Day + SLS + Sandbox skrócony.
Wojewódzki Ośrodek Medycyny Pracy w Opolu z/s w K-Koźlu – SIEDZIBA GŁÓWNA
ul. Mikołaja Reja 2A,
47-220 Kędzierzyn-Koźle
(dla 50 komputerów, 2 serwerów, + 2 NAS)

2 Minimum SN220 Security Pack + Next Business Day
Przychodnia Rejonowo - Profilaktyczna „PIASTOWSKA"
ul. Piastowska 51,
47-200 Kędzierzyn-Koźle
(dla 6 komputerów, 1 serwera)

3 Minimum SN220 Security Pack + Next Business Day
Ośrodek Rehabilitacyjny
ul. Aleja Jana Pawła II 31
47-220 Kędzierzyn-Koźle
(dla 2 komputerów)

Ad. 1 - DO SIEDZIBY GŁÓWNEJ

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe:

- Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
- System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 100/1000/2500.
- Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.11Q.
- W zakresie Firewall'a obsługa nie mniej niż 400 tys. jednoczesnych połączeń oraz 25 tys. nowych połączeń na sekundę.
- System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
- System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 256 GB lub pozwalać na zbieranie logów na zewnętrznym dysku, pendrive lub karcie MicroSD o pojemności co najmniej 256 GB do celów logowania i raportowania.
- W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:

    - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
    - Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, FTP).
    - System AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.
    - Poufność danych - IPSec VPN oraz SSL VPN
    - Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
    - Kontrola stron Internetowych – Web Filtering
    - Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
    - Kontrola pasma oraz ruchu [QoS i Traffic shaping]
    - Kontrola aplikacji oraz rozpoznawanie ruchu P2P
    - Analiza ruchu szyfrowanego protokołem SSL

- Wydajność systemu Firewall minimum 8 Gbps
- Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus minimum 1 Gbps
- Wydajność ochrony przed atakami (IPS) minimum 4 Gbps
- Wydajność VPN IPSec przy szyfrowaniu AES nie mniej niż 2 Gbps
- Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP.
- Urządzenie ma posiadać filtr URL.
- Urządzenie ma być dostarczone wraz z komercyjnym, europejskim skanerem Antywirusowym oraz umożliwiać skanowanie plików w oparciu o Sandboxing zlokalizowany w Internecie na serwerach producenta. Nie dopuszcza się aby analiza była przeprowadzana na urządzeniu

lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza była przeprowadzana przez firmy trzecie.

- Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
- Urządzenie ma posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. Moduł musi działać na urządzeniu. Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci. Powyższy moduł ma nie tylko wykrywać oprogramowanie ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu.
- Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowy. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu.
- W zakresie realizowanych funkcjonalności systemu raportowania i przeglądania logów, wymagane jest nie mniej niż:

    - Posiadanie predefiniowanych raportów dla ruchu WWW, modułu IPS, skanera antywirusowego i antyspamowego
    - Generowanie co najmniej 25 różnych typów raportów

- Urządzenie musi:

    - posiadać **certyfikat Common Criteria EAL**
    - posiadać **certyfikat ICSA Labs dla funkcji: VPN IPSec** lub znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE

Wraz z rozwiązaniem wykonawca musi dostarczyć system logowania i raportowania, korelujący zdarzenia i generujący raporty na podstawie danych z systemów bezpieczeństwa.

- System musi zostać dostarczony w postaci maszyny wirtualnej instalowanej w środowisku Vmware lub Windows Hyper-V.
- Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów
- Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP.
- Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS.
- Rozwiązanie musi umożliwiać przesyłanie logów do innego serwera logów (funkcja syslog forwarder).
- Rozwiązanie jest lokalne i wymaga instalacji w środowisku klienta
- Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP,GeoIP)
- Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie.
- Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.).
- Rozwiązanie musi umożliwiać na podstawie kryteriów przeszukiwania logów tworzenie reguły alarmującej administratora. Reguła zostaje uaktywniona, gdy wszystkie kryteria zapytania zostaną spełnione. Powiadomienie musi mieć formę minimum wiadomości email.
- Rozwiązanie musi mieć funkcjonalność tworzenia incydentów z kryteriów zapytań i zarządzanie incydentami poprzez możliwość przypisywania osób do obsługi incydentów, komentowania incydentów, podejrzenia logów źródłowych które zawarte są w incydencie

- Liczba zdarzeń na sekundę (EPS): min. 10 000
- Zarządzanie logami: min 1 rok
- Liczba zapisu zdarzeń na dobę: min 13000 MB

Wymaga się, aby dostawa obejmowała również:

- Minimum **36-miesięczną gwarancję producentów** na dostarczone elementy systemu liczoną od dnia zakończenia wdrożenia całego systemu.
- Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres minimum **36 miesięcy** liczoną od dnia zakończenia wdrożenia całego systemu.
- **Rozszerzoną gwarancją typu NBD tzn. w przypadku zgłoszenia awarii urządzenia**, wysyłka urządzenia zastępczego lub wysyłka sprawnego urządzenia musi nastąpić w dniu potwierdzenia awarii, a dostawa takiego urządzenia na wskazany przez zgłaszającego adres zaplanowana zostanie na kolejny dzień roboczy. Posiadanie rozszerzonej gwarancji NBD musi zostać potwierdzone licencją dystrybutora/producenta. Podmiot realizujący rozszerzoną gwarancję NBD musi posiadać certyfikat bezpieczeństwa informacji ISO27001 lub równoważny.

Ad. 2 i 3 - DO DWÓCH POZOSTAŁYCH JEDNOSTEK

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe:

- Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
- System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 100/1000/2500.
- Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.11Q.
- W zakresie Firewall'a obsługa nie mniej niż 300 tys. jednoczesnych połączeń oraz 20 tys. nowych połączeń na sekundę.
- System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
- System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 256 GB lub pozwalać na zbieranie logów na zewnętrznym dysku, pendrive lub karcie MicroSD o pojemności co najmniej 256 GB do celów logowania i raportowania.
- W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:

    - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
    - Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, FTP).
    - System AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.
    - Poufność danych - IPSec VPN oraz SSL VPN
    - Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]

- Kontrola stron Internetowych – Web Filter [WF]
- Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3)
- Kontrola pasma oraz ruchu [QoS i Traffic shaping]
- Kontrola aplikacji oraz rozpoznawanie ruchu P2P
- Analiza ruchu szyfrowanego protokołem SSL

- Wydajność systemu Firewall minimum 4 Gbps
- Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus minimum 500 Mbps
- Wydajność ochrony przed atakami (IPS) minimum 2 Gbps
- Wydajność VPN IPSec przy szyfrowaniu AES nie mniej niż 1 Gbps
- Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP.
- Urządzenie ma posiadać filtr URL.
- Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
- W zakresie realizowanych funkcjonalności systemu raportowania i przeglądania logów, wymagane jest nie mniej niż:

    - Posiadanie predefiniowanych raportów dla ruchu WWW, modułu IPS, skanera antywirusowego i antyspamowego
    - Generowanie co najmniej 25 różnych typów raportów

- Urządzenie musi:

    - posiadać certyfikat Common Criteria EAL
    - posiadać certyfikat ICSA Labs dla funkcji: VPN IPSec lub znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE

Wymaga się, aby dostawa obejmowała również:

- Minimum **36-miesięczną gwarancję producentów** na dostarczone elementy systemu liczoną od dnia zakończenia wdrożenia całego systemu.
- Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres **minimum 36 miesięcy** liczoną od dnia zakończenia wdrożenia całego systemu.
- Rozszerzoną **gwarancją typu NBD tzn. w przypadku zgłoszenia awarii urządzenia**, wysyłka urządzenia zastępczego lub wysyłka sprawnego urządzenia musi nastąpić w dniu potwierdzenia awarii, a dostawa takiego urządzenia na wskazany przez zgłaszającego adres zaplanowana zostanie na kolejny dzień roboczy. Posiadanie rozszerzonej gwarancji NBD musi zostać potwierdzone licencją dystrybutora/producenta. Podmiot realizujący rozszerzoną gwarancję NBD musi posiadać certyfikat bezpieczeństwa informacji ISO27001 lub równoważny.

ZAKRES ZAMÓWIENIA OBEJMUJE:

Oferta powinna zawierać urządzenia **STORMSHIELD spełniające w/w warunki** wraz z elementami wdrożenia na miejscu w jednostkach w których zakresie będzie:

- Przygotowanie infrastruktury
- Aktualizacja oprogramowania (opcjonalnie)
- Konfiguracja urządzenia wraz z przeszkoleniem pracownika w danym segmencie obsługi oprogramowania jak i urządzenia.
- Konfiguracja max 4 portów LAN/WAN
- W ramach konfiguracji 4 portów LAN/WAN konfiguracja load balancingu
- Konfiguracja profili bezpieczeństwa (IPS)
- Konfiguracja do 15 polityk bezpieczeństwa (reguł firewall)
- Konfiguracja 5 reguł NAT
- Utworzenie do 20 obiektów
- Konfiguracja tuneli VPN Site To Site pomiędzy jednostkami
- Konfiguracja urządzenia w trybie routera (NAT) lub w trybie transparentnym
- Stworzenie reguł URL filteringu
- Konfiguracji w trybie transparentnym (bez konfiguracji usług zewnętrznych np. IP SEC VPN)
- Udzielanie wsparcia powdrożeniowego co najmniej przez okres trwania okresu licencjonowania

CERTYFIKATY WYKONAWCZE

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy dysponują wskazanymi zasobami tj. minimum dwóch pracownik wdrażających rozwiązanie z certyfikatem producenta: **Certified Stormshield Network Expert** w tym minimum jeden pracownik wdrażający rozwiązanie z certyfikatem producenta: **Certified Stormshield Network Troubleshooting & Support**

3.2. ZADANIE II – OPIS

Dostarczenie systemów z dziedziny przygotowywania backupa danych (kopi zapasowych danych) w postaci urządzeń dla siedziby głównej Wojewódzkiego Ośrodka Medycyny Pracy w Opolu z/s w Kędzierzynie-Koźlu przy ulicy Mikołaja Reja 2A. Dostarczony system kopii zapasowych ma opierać się na urządzeniu marki **QNAP TS-1264U-RP-8G,** a z nim dostarczone powinny zostać **szyny RAIL-B02** jak i dyski **WD Red Plus WD80EFPX 8TB SATA (6 sztuk).** Do tak przygotowanego urządzenia dodatkowo chcielibyśmy zakupić oprogramowanie do backupu Xopero w wersji bezterminowej z co najmniej rocznym serwisem. Oprogramowanie powinno umożliwiać zgrywanie danych i tworzenie kopi co najmniej 3 serwerów Windows Server.

ZAKRES ZAMÓWIENIA OBEJMUJE:

Oferta powinna zawierać następujące składniki i urządzenia:

Lp.	Nazwa
1	TS-1264U-RP-8G
2	Szyny RAIL-B02
3	WD Red Plus WD80EFPX 8TB SATA (6 sztuk)
4	Xopero One Server Agent (dla 3 serwerów)

wraz z elementami montażu i wdrożenia na miejscu w jednostce w których zakresie będzie:

- Przygotowanie infrastruktury
- Aktualizacja oprogramowania (opcjonalnie)
- Konfiguracja urządzenia wraz z przeszkoleniem pracownika w danym segmencie obsługi oprogramowania jak i urządzenia.
- Udzielanie wsparcia powdrożeniowego co najmniej przez okres trwania okresu licencjonowania.

4. SPOSÓB, MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERTY

1. Oferent nie przewiduje podziału przedmiotu zamówienia dlatego oferty muszą obejmować **zadanie nr I i II**.
2. Złożyć oferty można w siedzibie zamawiającego indywidualnie w sekretariacie, przesłać pocztą lub też drogą elektroniczną (skan) na adres e-mail: sekretariat@womp.opole.pl, oraz dodatkowo na drugi adres DW na ppeljan@womp.opole.pl. Przy wyborze metody elektronicznej – proszę o nadanie tematu wiadomości: „**OFERTA IT”** oraz informację telefoniczną o wysyłce oferty i potwierdzenie w sekretariacie wydruku w/w oferty tel. 77/483 77 32 do dnia 2024-09-23 do godz. 12:00.
3. Otwarcie ofert nastąpi w obecności Wykonawców, którzy zechcą przybyć w dniu 2024-09-25 o godz. 9:00, do siedziby Zamawiającego, sala konferencyjna.

5. TERMIN REALIZACJI ZAMÓWIENIA

Od dnia podpisania umowy do **01.11.2024 r.**

6. OPIS SPOSOBU OBLICZANIA CENY

1. Podane w ofercie ceny muszą uwzględniać wszystkie wymagania ZAMAWIAJĄCEGO określone w niniejszej specyfikacji oraz obejmować wszelkie koszty, jakie poniesie Wykonawca z tytułu należytego oraz zgodnego z umową i obowiązującymi przepisami wykonania przedmiotu zamówienia.

2. Cenę oferty należy określić z dokładnością do dwóch miejsc po przecinku w następujący sposób:

ZADANIE I

Cena netto : .....

Podatek VAT: .....

Cena brutto : .....

ZADANIE II

Cena netto : .....

Podatek VAT: .....

Cena brutto : .....

Cena oferty winna obejmować wszystkie koszty realizacji przedmiotu zamówienia określonego w niniejszej zapytaniu ofertowym, w tym również wszelkie koszty towarzyszące wykonaniu zamówienia oraz wszelkie opłaty i podatki.

7. KRYTERIA OCENY OFERT (wyboru wykonawcy)

Nr:	Nazwa kryterium:	Waga:
1	Cena (Zadanie I + Zadanie II)	100

8. WYKLUCZENIE Z UDZIAŁU W POSTEPOWANIU

1. Zamawiający wykluczy Wykonawcę, który jest powiązany z Zamawiającym osobowo lub kapitałowo. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przeprowadzeniem procedury wyboru wykonawcy a Wykonawcą, polegające w szczególności na:

a. uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej;
b. posiadaniu co najmniej 10% udziałów lub akcji;
c. pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;
d. pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.

Zamawiający, w celu potwierdzenia braku powiązań osobowych lub kapitałowych, wymaga przedłożenia przez Wykonawcę oświadczenia (wzór oświadczenia stanowi Załącznik nr 1 do Zapytania ofertowego).

9. INFORMACJE DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH

Ochrona danych osobowych osób fizycznych i klauzula informacyjna z art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), zwane dalej „rozporządzeniem 2016/679".

1. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:
   a) administratorem Pani/Pana danych zbieranych i przetwarzanych w celu wyboru wykonawcy, zawarcia umowy oraz realizacji umowy jest Wojewódzki Ośrodek Medycyny Pracy w Opolu z/s w Kędzierzynie-Koźlu ul. Mikołaja Reja 2a, 47-220 Kędzierzyn-Koźle, Tel. 77 4837732 lub kom. 789462403., e-mail: sekretariat@womp.opole.pl,
   b) Dane osobowe mogą zostać ujawnione właściwym organom oraz podmiotom upoważnionym zgodnie z obowiązującym prawem.
   c) Osobom, które w ofercie podały swoje dane osobowe przysługuje prawo wglądu do treści tych danych oraz ich poprawienia. Podanie danych jest dobrowolne, ale konieczne dla wyboru wykonawcy, zawarcia umowy oraz realizacji umowy.
   d) Osobom, które w ofercie podały swoje dane osobowe przysługuje prawo do wniesienia sprzeciwu wobec dalszego przetwarzania.
   e) Osobom, które w ofercie podały swoje dane osobowe przysługuje prawo wniesienia skargi do organu nadzorczego.
   f) W przypadku, gdy przed zawarciem umowy zgłoszenie żądania ograniczenia przetwarzania, o którym mowa w art. 18 ust. 1 rozporządzenia 2016/679 wpływa na zmianę treści złożonej oferty, w sposób mający lub mogący mieć wpływ na wynik postępowania, zamawiający odrzuca ofertę zawierającą dane osobowe, których przetwarzanie ma zostać ograniczone.
   g) Dane osobowe są przetwarzane na podstawie art. 6 ust. 1 lit c rozporządzenia 2016/679.
   h) Okres przetwarzania danych jest zgodny z kategorią archiwalną dokumentacji postępowania.
   i) Dane kontaktowe do Inspektora Ochrony Danych – sekretariat@womp.opole.pl, tel. 77 4837732.

2. W przypadku przekazywania Zamawiającemu danych osobowych w sposób inny niż od osoby, której dane dotyczą, Wykonawca zobowiązany jest do podania osobie, której dane dotyczą informacji, o których mowa w art. 14 rozporządzenia 2016/679

10. SPOSÓB KONTAKTOWANIA SIĘ Z ZAMAWIAJĄCYM

Osobą udzielającą informacji w zakresie niniejszego zapytania ofertowego jest informatyk

Piotr Peljan:
tel. 77 4837732
email: ppeljan@womp.opole.pl

11. ISTOTNE POSTANOWIENIA UMOWY

Wzór umowy stanowi Załącznik nr 2

12. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

1) Oferta musi być sporządzona w języku polskim, w formie pisemnej pod rygorem nieważności.
2) Oferta musi zawierać:

- dane oferenta,
- oferowany przedmiot zamówienia (zadanie I i II),
- cenę netto i brutto przedmiotu zmówienia z podziałem na zadanie (I i II),
- cena powinna obejmować wszystkie koszty: urządzeń, dostawy, montażu, wdrożenia uruchomienia, oprogramowania),
- proponowany okres gwarancji,
- czas realizacji zamówienia (do 01.11.2024r.).

3) Oświadczenie o niepodleganiu wykluczeniu - wg załącznika nr 1 do niniejszego zapytania.

13. UDZIELENIE ZAMÓWIENIA

1. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w niniejszym zapytaniu i została oceniona jako najkorzystniejsza w oparciu o podane wyżej kryteria oceny ofert.
2. Zamawiający może unieważnić postępowanie na każdym jego etapie bez podania przyczyny.
3. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający jednocześnie zawiadomi Wykonawców, którzy złożyli oferty, o wyborze najkorzystniejszej oferty, podając nazwę (firmę), albo imię i nazwisko, siedzibę albo adres zamieszkania i adres wykonawcy, którego ofertę wybrano.

4. Ogłoszenie zawierające informacje wskazane w pkt 3 Zamawiający umieści na stronie internetowej oraz w miejscu publicznie dostępnym w swojej siedzibie głównej.

Sporządził dn. 06.09.2024r.

……

Zatwierdził dn. 06.09.2024r.

……