Związek Gmin Regionu Płockiego
razem od 1994 roku

Bielsk, Bodzanów, Brudzeń Duży, Bulkowo, Czerwińsk nad Wisłą, Drobin, Gąbin, Gmina Gostynin, Łąck, Mała Wieś, Nowy Duninów, Pacyna, Płock, Radzanowo, Słupno, Stara Biała, Staroźreby, Szczawin Kościelny, Wyszogród

Nr sprawy ZAO-AO.271.6.2018.RM

Płock, dnia 18.04.2018r.

ZAPROSZENIE DO PRZEDSTAWIENIA OFERTY CENOWEJ

Związek Gmin Regionu Płockiego informuje iż niniejsze zaproszenie posłuży Zamawiającemu do obliczenia wartości szacunkowej zamówienia i może stanowić ofertę w rozumieniu przepisów art. 4 pkt 8 Ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t. j. Dz. U. z 2017 r. poz. 1579 z późn. zm.)

Zamawiający Związek Gmin Regionu Płockiego ul. Zglenickiego 42, 09-411 Płock, zaprasza do składania ofert w postępowaniu o wartości zamówienia nieprzekraczającej kwot określonych w art. 4 pkt 8 ustawy Prawo zamówień publicznych w celu wyboru najkorzystniejszej oferty na zakup i dostawę oprogramowania antywirusowego dla stacji roboczych i serwerów:

1) oprogramowanie antywirusowe dla stacji roboczych i serwerów – ***ilość: sztuk 60,***

I. Zamawiający

Związek Gmin Regionu Płockiego, ul. Zglenickiego 42, 09-411 Płock, Budynek S

II. Tryb postępowania

Zapytanie ofertowe na podstawie art. 4 pkt 8 Ustawy Prawo zamówień publicznych (t. j. Dz. U. z 2017 r. poz. 1579 z późn. zm.)

III. Kod CPV zamówienia

48761000-0 – Pakiety oprogramowania antywirusowego

IV. Przedmiot Zamówienia

1. Przedmiotem Zamówienia jest zakup i dostawa oprogramowania antywirusowego dla stacji roboczych i serwerów w ilości szt. 60 spełniającego poniższe parametry techniczne:

1) **Wymagania ogólne:**

- Pełne wsparcie dla systemów zainstalowanych na stacjach roboczych Windows Vista/Windows7 /Windows8 / Windows, w ilości sztuk 55 stacji roboczych ,
- Pełne wsparcie dla zainstalowanych systemów serwerowych Windows Server 2012, Windows Server 2016, w ilości sztuk 2 serwerów z systemem Windows Server,
- Pełne wsparcie dla zainstalowanych systemów serwerowych Linux Debian, w ilości sztuk stacji 3 serwerów z systemem Linux Debian,
- Wsparcie dla 32 i 64 – bitowej architektury wersji systemów Windows i Linux,
- Wersja oprogramowania dla systemów Windows dostępna będzie zarówno w języku polskim jak i angielskim,
- Pomoc w programie (help) dla systemów Windows i dokumentacja do programu w języku polskim.

2) **Wymagania dotyczące ochrony antywirusowej i antyspyware:**

- Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami,
- Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.,
- Wbudowana technologia do ochrony przed rootkitami,
- Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików,
- Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu,
- Oferowane rozwiązanie ma umożliwić administratorowi definiowanie zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało, czy komputer pracuje na zasilaniu bateryjnym, jeśli komputer pracuje na zasilaniu bateryjnym zadanie powinno pozostać niewykonane,
- Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania),
- Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym,
- Możliwość skanowania dysków sieciowych i dysków przenośnych,

- Skanowanie plików spakowanych i skompresowanych,
- Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń),
- Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach,
- Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu,
- Brak wymogu od użytkownika, ponownego uruchomienia komputera, po włączeniu ochrony antywirusowej,
- Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny), w celu dalszej kontroli,
- Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird od wersji 5.x i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego),
- Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird od wersji 5.x i Windows Live Mail, będących w użytkowaniu przez Zamawiającego,
- Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego),
- Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym, bez konieczności zmian w konfiguracji,
- Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie,
- Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail,
- Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie,
- Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony,

- Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora,
- Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji,
- Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie,
- Skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS,
- Skanowanie ruchu HTTPS transparentnie, bez potrzeby konfiguracji zewnętrznych aplikacji takich, jak przeglądarki Web lub programy pocztowe,
- Funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika,
- Procesy zweryfikowane, jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym,
- Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe,
- Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta,
- Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze, przy próbie dostępu do konfiguracji był poproszony o podanie hasła,
- Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet wówczas, gdy posiada ona prawa lokalnego użytkownika, bez nadanych uprawnień specjalnych,
- Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: stacji dyskietek, napędów CD/DVD, czytników kart, urządzeń Bluetooth, portów LPT/COM oraz portów USB,
- Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model,
- Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia,
- W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika,

- Program musi być wyposażony w system zapobiegania włamaniom działającym na hoście (HIPS),
- Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu,
- Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami,
- Aplikacja musi być wyposażona w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji, w celu ich późniejszego przywrócenia (rollback),
- Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania,
- Wsparcie techniczne do programu ma być świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.

3) **Wymagania dotyczące centralnego zarządzania:**

- Darmowe oprogramowanie centralnego zarządzania, zainstalowane na serwerze Zamawiającego z Windows Server 2012 R2 Standard o architekturze 64-bitowej,
- Centralna instalacja programów, służących do ochrony stacji roboczych Windows, Linux użytkowanych przez Zamawiającego,
- Centralne zarządzanie programami służącymi, do ochrony stacji roboczych,
- Centralna instalacja oprogramowania na końcówkach (stacjach roboczych) z systemami operacyjnymi typu Windows Vista/Windows7/Windows 8/Windows 10, będących w użytkowaniu przez Zamawiającego,
- Do instalacji centralnej i zarządzania centralnego nie jest wymagana dodatkowa aplikacja (agent). Na końcówkach zainstalowany jest sam program antywirusowy,
- Komunikacja miedzy serwerem, a klientami może być zabezpieczona hasłem,
- Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową i kontrolą dostępu do stron internetowych, zainstalowanymi na stacjach roboczych w sieci,
- Możliwość uruchomienia centralnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej,
- Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie),

- Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacja robocza należy,
- Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu,
- Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych,
- Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnych dla zarządzanych programów,
- Możliwość importowania konfiguracji programu z wybranej stacji roboczej, a następnie przesłanie (skopiowanie) jej na inną stację lub grupę stacji roboczych w sieci,
- Możliwość uruchomienia serwera centralnej administracji i konsoli zarządzającej na stacjach Windows Vista/Windows 7/Windows 8/ Widows 10 oraz na serwerach 2012 i 2016 – 32 i 64 -bitowe systemy, będących w użytkowaniu przez Zamawiającego,
- Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie żadnych dodatkowych baz typu MSDE lub MS SQL. Serwer centralnej administracji musi mieć własną wbudowaną bazę,
- Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) w formacie HTML lub CSV,
- Aplikacja musi posiadać funkcjonalność, która umożliwi przesłanie wygenerowanych raportów na wskazany adres e-mail,
- Do wysłania raportów aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na stacji gdzie jest uruchomiona usługa serwera,
- Serwer centralnej administracji ma oferować funkcjonalność synchronizacji grup komputerów z drzewem Active Directory. Po synchronizacji automatycznie są umieszczane komputery należące do zadanych grup w AD do odpowiadających im grup w programie,
- Serwer centralnej administracji ma być wyposażony w mechanizm informowania administratora o wykryciu nieprawidłowości w funkcjonowaniu oprogramowania zainstalowanego na klientach, w tym przynajmniej informowaniu o: wygaśnięciu licencji na oprogramowanie o tym, że zdefiniowany procent spośród wszystkich stacji podłączonych do serwera ma nieaktywną ochronę oraz, że niektórzy z klientów podłączonych do serwera oczekują na ponowne uruchomienie po aktualizacji do nowej wersji oprogramowania,
- Serwer centralnej administracji ma być wyposażony w wygodny mechanizm zarządzania licencjami, który umożliwi sumowanie liczby licencji nabytych przez użytkownika. Dodatkowo

serwer ma informować o tym, ilu stanowiskową licencję posiada użytkownik i stale nadzorować, ile licencji spośród puli nie zostało jeszcze wykorzystanych,

- W sytuacji, gdy użytkownik wykorzysta wszystkie licencje, które posiada po zakupie oprogramowania, administrator po zalogowaniu się do serwera poprzez konsolę administracyjną musi zostać poinformowany, o tym fakcie za pomocą okna informacyjnego,
- Aplikacja musi posiadać funkcjonalność, która umożliwi dystrybucję aktualizacji za pośrednictwem szyfrowanej komunikacji (za pomocą protokołu https),
- W celu aktualizacji za pośrednictwem protokołu https, nie jest wymagane instalowanie dodatkowych zewnętrznych usług,
- Dostęp do kwarantanny klienta ma być możliwy z poziomu systemu centralnego zarządzania,
- Możliwość przywrócenia lub pobrania zainfekowanego pliku ze stacji klienckiej przy wykorzystaniu centralnej administracji,
- Administrator ma mieć możliwość przywrócenia i wyłączenia ze skanowania pliku pobranego z kwarantanny stacji klienckiej,
- Podczas przywracania pliku, administrator ma mieć możliwość zdefiniowania kryteriów dla plików, które zostaną przywrócone, w tym minimum: zakres czasu z dokładnością co do minuty, kiedy wykryto daną infekcję, nazwa danego zagrożenia, dokładna nazwa wykrytego obiektu oraz zakres minimalnej i maksymalnej wielkości pliku z dokładnością do jednego bajta,
- Możliwość definiowania administratorów o określonych prawach do zarządzania serwerem administracji centralnej (w tym możliwość utworzenia administratora z pełnymi uprawnieniami lub uprawnienia tylko do odczytu),
- W przypadku tworzenia administratora z niestandardowymi uprawnieniami, możliwość wyboru modułów, do których ma mieć uprawnienia: zarządzanie grupami, powiadomieniami, politykami, licencjami oraz usuwanie i modyfikacja klientów, zdalna instalacja, generowanie raportów, usuwanie logów, zmiana konfiguracji klientów, aktualizacja zdalna, zdalne skanowanie klientów, zarządzanie kwarantanną na klientach,
- Możliwość synchronizowania użytkowników z Active Directory, w celu nadania uprawnień administracyjnych do serwera centralnego zarządzania,
- Wszystkie działania administratorów zalogowanych do serwera administracji centralnej mają być logowane,
- Możliwość uruchomienia panelu kontrolnego dostępnego za pomocą przeglądarki internetowej,
- Panel kontrolny musi umożliwiać administratorowi wybór elementów monitorujących, które mają być widoczne,

- Elementy monitorujące muszą umożliwiać podgląd w postaci graficznej, co najmniej: bieżącego obciążenia serwera zarządzającego, statusu serwera zarządzającego, obciążenia bazy danych, z której korzysta serwer zarządzający, obciążenia komputera, na którym zainstalowana jest usługa serwera zarządzającego, informacji odnośnie komputerów z zainstalowaną aplikacją antywirusową, a które nie są centralnie zarządzane, podsumowania modułu antyspamowego, informacji o klientach znajdujących się w poszczególnych grupach, informacji o klientach z największą ilością zablokowanych stron internetowych, klientach, na których zostały zablokowane urządzenia zewnętrzne, zagrożeń oraz ataków sieciowych,
- Administrator musi posiadać możliwość maksymalizacji wybranego elementu monitorującego,
- Możliwość włączenia opcji pobierania aktualizacji z serwerów producenta z opóźnieniem,
- Wsparcie dla protokołu IPv6,
- Administrator musi posiadać możliwość centralnego, tymczasowego wyłączenia wybranego modułu ochrony na stacji roboczej,
- Centralne tymczasowe wyłączenie danego modułu nie może skutkować koniecznością restartu stacji roboczej,
- Aplikacja musi posiadać możliwość natychmiastowego uruchomienia zadania, znajdującego się w harmonogramie bez konieczności oczekiwania do jego zaplanowanego czasu.

4) Wymagania, dotyczące wsparcia technicznego:

- Pobieranie aktualizacji programu oraz poprawek do działania programu ze strony producenta oprogramowania lub Wykonawcy,
- Pobieranie uaktualnień baz programu z sygnaturami wirusów oraz szczepionek,
- Korzystanie ze strony internetowej producenta programu,
- Pomoc w rozwiązywaniu problemów technicznych w działaniu programu przez Wykonawcę oraz serwis techniczny producenta oprogramowania, w tym rozwiązywanie problemów konfiguracyjnych związanych ze sprawnym funkcjonowaniem komputerów we współpracy z programem,
- Instruktaż w zakresie obsługi programu na żądanie Zamawiającego,
- Udzielanie pracownikom Zamawiającego konsultacji telefonicznych.

5) **Wymagania dotyczące serwisu, aktualizacji i instruktaży:**

- W całym okresie objętym umową, Zamawiający będzie miał prawo do korzystania z bezpłatnej pomocy technicznej zapewnionej przez Wykonawcę,
- W całym okresie objętym umową, Zamawiający będzie miał prawo do pobierania i instalacji nieodpłatnie nowszych wersji w ramach posiadanej licencji,
- W całym okresie objętym umową, Zamawiający będzie miał prawo do nieodpłatnego korzystania z uaktualnień baz z sygnaturami wirusów oraz szczepionek.

6) **Wymagania dotyczące licencji na Przedmiot Zamówienia:**

- Dokument licencji na oprogramowanie, obejmujący 60 sztuk licencji powinien zostać złożony w wersji papierowej w siedzibie Zamawiającego osobiście lub za pośrednictwem poczty tradycyjnej i/lub przesyłki kurierskiej,
- Klucz licencyjny na oprogramowanie, obejmujący 60 sztuk licencji powinien zostać przesłany w wersji elektronicznej na skrzynkę pocztową wskazaną przez Zamawiającego,
- Adres strony internetowej, z której można pobrać oprogramowanie powinien zostać przesłany w wersji elektronicznej na skrzynkę pocztową wskazaną przez Zamawiającego,
- Dokument licencji powinien uprawniać do 24-miesięcznego wsparcia technicznego oraz aktualizacji programu, baz antywirusowych oraz szczepionek,
- Zamawiający ustala adres skrzynki, przeznaczonej do wymiany dokumentów wymienionych w niniejszym punkcie jako adres it@zgrp.pl.

V. Forma i miejsce składania ofert

Ofertę należy złożyć drogą elektroniczną na adres e-mail: it@zgrp.pl, w ofercie podając cenę netto i brutto.

VI. Warunki udziału w postępowaniu

- Wykonawca znajduje się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia,
- Wykonawca dysponuje potencjałem technicznym i osobowym, zdolnym do wykonania zamówienia,
- Wykonawca zapewnia, iż złożona oferta będzie w 100% spełniała warunki zaproszenia do składania ofert,

- Wykonawca przedstawi ofertę na oprogramowanie antywirusowe z ważną 24-miesięczną licencją, na wszystkie funkcjonalności określone w pkt IV niniejszego zapytania ofertowego,
- Wykonawca zapewnia, iż Przedmiot Zamówienia dostarczony w ramach zamówienia jest nowy i wolny od wad oraz pochodzi z oficjalnego punktu dystrybucyjnego,
- Wykonawca udzieli gwarancji na zakupiony Przedmiot Zamówienia, którego parametry techniczne opisane są w pkt IV niniejszego Zapytania Ofertowego,
- Koszt dostawy Przedmiotu Zamówienia do Biura Związku Gmin Regionu Płockiego pokrywa Wykonawca,
- Wykonawca wystawi fakturę VAT po przedłożeniu protokołu zdawczo – odbiorczego,
- Zamawiający zastrzega sobie, iż w chwili rezygnacji z dostawy Przedmiotów Zamówienia przez Wykonawcę, który złożył najkorzystniejszą ofertę, Zamawiający udzieli realizację dostawy Przedmiotów Zamówienia Wykonawcy, którego oferta cenowa uzyskała drugie miejsce w ocenie ofert,
- Zamawiający zastrzega sobie zmianę ilości sztuk Przedmiotów Zamówienia, mając jednocześnie na myśli zwiększenie bądź zmniejszenie ilości sztuk lub całkowitą rezygnację z Przedmiotu Zamówienia po oszacowaniu zamówienia na podstawie niniejszego postępowania,
- Wykonawca składając ofertę cenową na Przedmiot Zamówienia określone w pkt IV niniejszego zapytania ofertowego, powinien załączyć szczegółową specyfikację techniczną producenta przedmiotu do przedstawianej oferty cenowej.

VII. Zamawiający przy wyborze najkorzystniejszej oferty będzie kierował się kryteriami, dla których przypisał poszczególne wagi:

1. Cena;

   Kryterium: „Cena" 80% – Cena będzie rozpatrywana na podstawie ceny brutto za wykonanie Przedmiotu Zamówienia, podanej przez Wykonawcę w formularzu ofertowym.

   W przypadku kryterium **„Cena",** oferta otrzyma zaokrągloną do dwóch miejsc po przecinku liczbę punktów wynikającą z działania:

   $$C = C_{min}/C_b \times 100 = ...pkt$$

   gdzie,

   C – liczba punktów, jakie otrzymała oferta badana za kryterium „Cena",

   C_{min} – najniższa cena brutto spośród wszystkich ważnych ofert,

   C_b – cena brutto oferty badanej.

2. Czas realizacji zamówienia;

Kryterium „Czas realizacji zamówienia" 20% – Punkty za kryterium „Czas realizacji zamówienia" Przedmiotu Zamówienia – zostaną przyznane według następujących zasad:

- od 1 do 7 dni kalendarzowych – Zamawiający przyzna 20 pkt,

- od 8 do 14 dni kalendarzowych – Zamawiający przyzna 10 pkt,

- powyżej 14 dni kalendarzowych - Zamawiający przyzna 0 pkt.

Za najkorzystniejszą ofertę cenową zostanie uznana ta z największą ilością punktów, stanowiących sumę punktów przyznanych w każdym kryterium z uwzględnieniem wagi procentowej danego kryterium obliczonego ze wzoru:

$$P = C \times 80\% + R\ 20\%$$

gdzie:

P – łączna ilość punktów przyznana ofercie badanej,

C – ilość punktów przyznana ofercie ocenionej z kryterium „Cena",

R – ilość punktów przyznana ofercie ocenionej z kryterium „Czas realizacji zamówienia".

VIII. Opis sposobu przygotowania oferty:

1. Ofertę należy złożyć na **formularzu ofertowym** - załącznik nr 1 do Zapytania Ofertowego.
2. Ofertę należy przesłać do dnia 26.04.2019 r. do godziny 16:00 na adres e-mail: it@zgrp.pl z dopiskiem w temacie wiadomości „**Oprogramowanie antywirusowe ZGRP**".
3. Wykonawca przedstawi ofertę, której treść musi odpowiadać treści Zapytania Ofertowego.
4. Oferta powinna być podpisana przez osobę upoważnioną do reprezentowania Wykonawcy (data i podpis).
5. Oferty niekompletne, nieczytelne lub złożone po terminie nie będą rozpatrywane.

IX. Osoby upoważnione do porozumiewania się z Wykonawcami

Rafał Mieszkowski – Informatyk Biura Związku Gmin Regionu Płockiego - Koordynator Zespołu IT, tel. 24 366 04 27, e-mail: r.mieszkowski@zgrp.pl oraz Krzysztof Hejcelman –Samodzielny referent ds. IT tel. 24 366 04 27, e-mail: k.hejcelman@zgrp.pl

X. Odrzucenie ofert

Wykonawca zostanie odrzucony z niniejszego postępowania:

1. w przypadku niespełnienia warunków udziału w postępowaniu,
2. w przypadku niezgodności oferty z niniejszym zapytaniem.

XI. Unieważnienie postępowania

Zamawiający zastrzega sobie możliwość unieważnienia postępowania, bez podania przyczyny na każdym etapie postepowanie.

XII. Pozostałe informacje

1. Zamawiający zastrzega sobie możliwość zmiany lub uzupełnienie treści Zapytania Ofertowego, przed upływem terminu na składanie ofert. Informacja o wprowadzeniu zmiany lub uzupełnieniu treści Zapytania Ofertowego zostanie umieszczona w Biuletynie Informacji Publicznej Związku Gmin Regionu Płockiego (http://zgrp.bip.org.pl).
2. Jeżeli wprowadzone zmiany lub uzupełnienia treści Zapytania Ofertowego będą wymagały zmiany treści ofert, Zamawiający przedłuży termin składania ofert o czas potrzebny na dokonanie zmian w ofercie.
3. Zamawiający zawrze umowę (wzór umowy stanowi załącznik nr 2 do niniejszego Zapytania Ofertowego) z Wykonawcą, którego oferta zostanie uznana za ofertę najkorzystniejszą oraz, który spełni wymogi określone w Zapytaniu Ofertowym. O terminie zawarcia Umowy Zamawiający powiadomi Wykonawcę drogą e-mailową wraz z informacją o wynikach postępowania.
4. Jeżeli Zamawiający nie może dokonać wyboru oferty najkorzystniejszej ze względu na to, że zostały złożone oferty o takiej samej cenie (otrzymały taką samą liczbę punktów), Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego, ofert dodatkowych.
5. Zamawiający dopuszcza udzielenie zamówienia dodatkowego w wysokości nie większej niż 20% zamówienia podstawowego.

XIII. Wykaz załączników

Załącznik nr 1 – Formularz Ofertowy

Załącznik nr 2 – Wzór Umowy

Katarzyna Rogucka-Maciejowska

Dyrektor Biura
Związku Gmin Regionu Płockiego

Z poważaniem

Sporządził: Rafał Mieszkowski tel. 24 366 04 27 e-mail: r.mieszkowski@zgrp.pl