GK.272.3.58.2024 Data: 25.11.2024r.

ZAPYTANIE OFERTOWE

GMINA PAPOWO BISKUPIE
Adres: Papowo Biskupie 128, 86-221 Papowo Biskupie

na Zakup oprogramowania XDR dla Urzędu Gminy Papowo Biskupie na okres 24 miesięcy
o wartości szacunkowej nieprzekraczającej kwoty 130 000,00 zł, o której mowa w art. 2 ust. 1 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. 2024 poz. 1320 z późn. zm.)

Zamawiający: GMINA PAPOWO BISKUPIE,
Adres: Papowo Biskupie 128, 86-221 Papowo Biskupie, NIP 875-148-68-52

I.	**Opis przedmiotu zamówienia Urząd Gminy** Aktualizacja (upgrade) oprogramowania zabezpieczającego końcowe stacje komputerowe oraz serwery - ESET Identyfikator licencji: **33B-JTG-UA4** wygasa w dniu **25.01.2025r**. okres przedłużenia licencji: **24 miesiące** liczba licencji: **40** uwaga: **prawo do korzystania z zakupionej puli ma również GOPS**
II.	**Termin i miejsce wykonania zamówienia.** Miejsce wykonania zamówienia: Urząd Gminy Papowo Biskupie Potwierdzeniem wykonania zamówienia jest podpisany protokół dostawy licencji oprogramowania i jego certyfikatu do dnia **31 grudnia 2024r.**

OPIS PRZEDMIOTU ZAMÓWIENIA

1. **Kod i nazwa według Wspólnego Słownika Zamówień:**

48760000-3 - Pakiety oprogramowania do ochrony antywirusowej
48761000-0 - Pakiety oprogramowania antywirusowego

2. Przedmiotem zamówienia jest aktualizacja (upgrade) oprogramowania zabezpieczającego końcowe stacje komputerowe oraz serwery - ESET PROTECT Enterprise, realizowanego w ramach Projektu grantowego pn. „Cyberbezpieczny Samorząd'' lub równoważnego zgodnie z zamieszczoną poniżej specyfikacją określającą minimalne parametry przedmiotu zamówienia.
3. **Minimalne parametry przedmiotu zamówienia:**

3.1. <u>Administracja zdalna w chmurze:</u>

1) W chmurze producenta.
2) Dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3) Zabezpieczenie za pośrednictwem protokołu SSL.
4) Mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5) Komunikacja agenta przy wykorzystaniu HTTP Proxy.

6) Zarządzanie urządzeniami mobilnymi – MDM.
7) Wymuszenie dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8) Dodanie zestawu uprawnień dla użytkowników w oparciu o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji ma możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9) 80 szablonów raportów, przygotowanych przez producenta.
10) Tworzenie grup statycznych i dynamicznych komputerów.
11) Grupy dynamiczne tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki zawierają: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12) Uruchamianie zadań automatycznie, z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

3.2. Ochrona stacji roboczych

1) Wsparcie systemów operacyjnych Windows (Windows 10/Windows 11).
2) Wsparcie architektury ARM64.
3) Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4) Wbudowana technologia do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5) Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6) Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7) Skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8) Skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9) Opcja umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10) Integracja z Intel Threat Detection Technology.
11) 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).
12) Skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13) Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Opcja wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14) Blokowanie zewnętrznych nośników danych na stacji w tym: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15) Blokowanie nośników wymiennych, bądź grup urządzeń umożliwia użytkownikowi tworzenie reguł dla podłączanych urządzeń w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16) Moduł HIPS ma możliwość pracy w jednym z pięciu trybów:

a) tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
b) tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
c) tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
d) tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program samoczynnie przełącza się w tryb pracy oparty na regułach,
e) tryb inteligentny, w którym powiadomienia będą wyłącznie o szczególnie podejrzanych zdarzeniach.
17) Wbudowana funkcja generująca pełny raport na temat stacji, na której zostało zainstalowane, z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
18) Funkcja, generująca taki log, posiada 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19) Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
20) Tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21) Skaner UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22) Ochrona antyspamowa dla programu pocztowego Microsoft Outlook.
23) Zapora osobista rozwiązania pracuje w jednym z czterech trybów:
a) tryb automatyczny –blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
b) tryb interaktywny – pyta się o każde nowo nawiązywane połączenie,
c) tryb oparty na regułach – blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
d) tryb uczenia się – automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator konfiguruje czas działania trybu.
24) Moduł bezpiecznej przeglądarki.
25) Przeglądarka automatycznie szyfruje wszelkie dane wprowadzane przez Użytkownika.
26) Praca w bezpiecznej przeglądarce jest wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27) Zintegrowany moduł kontroli dostępu do stron internetowych.
28) Filtrowanie adresów URL w oparciu o co 140 kategorii i podkategorii.
29) Ochrona przed zagrożeniami 0-day.
30) Na stacjach roboczych: wstrzymanie uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

3.3. Ochrona serwera

1) Wsparcie systemów Microsoft Windows Server 2012 i nowszych oraz Linux w tym: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.
2) Ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
3) Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

4) Skanowanie dysków sieciowych typu NAS.
5) Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Opcja wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6) Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
7) Wykluczanie ze skanowania procesów.
8) Określenie typu podejrzanych plików, jakie będą przesyłane do producenta, w tym pliki wykonywalne, archiwa, skrypty, dokumenty.
Dodatkowe funkcje dla ochrony serwerów Windows:
9) Skanowanie plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10) System zapobiegania włamaniom działający na hoście (HIPS).
11) Skanowanie magazynu Hyper-V.
12) Skaner UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13) Blokowanie zewnętrznych nośników danych na stacji w tym: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14) Automatyczne wykrywanie usług zainstalowanych na serwerze i tworzenie dla nich odpowiednich wyjątków.
15) Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16) Dodawanie wyjątków dla systemu IDS, w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17) Ochrona przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
Dodatkowe funkcje dla ochrony serwerów Linux:
18) Uruchamianie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
19) Lokalna konsola administracyjna nie wymaga do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20) Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, wspiera rozwiązanie Dell EMC Isilon.
21) Działa w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta zapewnia podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

3.4. Szyfrowanie

1) Instalacja aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
2) Wsparcie zarządzania natywnym szyfrowaniem w systemach macOS (FileVault).
3) Autentykacja typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Opcja całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4) Szyfrowanie danych tylko na komputerach z UEFI.

3.5. Sandbox w chmurze

1) Ochrona przed zagrożeniami 0-day.
2) Wykorzystywanie do działania chmury producenta.

3) Opcja określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4) Definiowanie po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5) Definiowanie maksymalnego rozmiaru przesyłanych próbek.
6) Tworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7) Po zakończonej analizie pliku, przesyłany jest wynik analizy do wszystkich wspieranych produktów.
8) Podgląd listy plików, które zostały przesłane do analizy.
9) Analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10) Brak wymogu instalacji dodatkowego agenta na stacjach roboczych.
11) Wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator ma podgląd jakie pliki zostały wysłane do analizy oraz przez kogo.
12) Przeanalizowane pliki są odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
a) Czysty,
b) Podejrzany,
c) Bardzo podejrzany,
d) Szkodliwy.
13) W przypadku stacji roboczych opcja wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
14) W przypadku serwerów pocztowych opcja wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15) Wykryte zagrożenia są przeniesione w bezpieczny obszar kwarantanny, z której można przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

3.6. Moduł EDR/XDR

1) Dostęp do konsoli centralnego zarządzania odbywa się z poziomu interfejsu WWW.
2) Wysyłanie zdarzeń do konsoli administracyjnej ESET.
3) Interfejs jest zabezpieczony za pośrednictwem protokołu SSL.
4) Wprowadzanie wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5) Wykluczenia dotyczą procesu lub procesu „rodzica”.
6) Utworzenie wykluczenia automatycznie rozwiązuje alarmy, które pasują do utworzonego wykluczenia.
7) Kryteria wykluczeń są konfigurowane w oparciu o: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8) Serwer posiada ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator może utworzyć własne reguły i edytować reguły dodane przez producenta.
9) Blokowanie plików po sumach kontrolnych. W ramach blokady można dodać komentarz oraz konfigurację wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
10) Weryfikacja uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.

11) W ramach plików wykonywalnych oraz plików DLL, opcja ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
12) Weryfikacja uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Oznaczanie skryptu jako bezpieczny lub niebezpieczny.
13) W ramach przeglądania wykonanego skryptu, możliwy szczegółowy podgląd wykonanych przez skrypt czynności w formie tekstowej.
14) W ramach przeglądania wykonanego skryptu lub pliku exe, możliwa weryfikacja powiązanych zdarzeń dotyczących: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
15) Przekierowanie do konsoli zarządzającej ESET, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli ESET, możliwy podgląd informacji dotyczącychj: podzespołów zarządzanego PC (w tym: producent, model, numer seryjny, informacje o systemie, procesor, peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
16) Tagowanie obiektów.
17) Połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

V. Kryteria wyboru oferty:

Cena brutto: 100% - kryterium oznacza najniższą cenę. Przyjmuje się, że 1% = 1 pkt i tak zostanie przeliczona liczba punktów. Ocena oferty w ramach niniejszego kryterium - cena brutto: będzie rozpatrywana na podstawie ceny brutto za wykonanie przedmiotu zamówienia (całkowitej, łącznej za wykonanie przedmiotu zamówienia), podanej przez Wykonawcę w Ofercie.

$$\text{Liczba punktów (max 100 pkt)} = \frac{\text{cena brutto oferty z najniższą ceną}}{\text{cena brutto oferty badanej}} \times 100$$

VI. Termin związania ofertą i płatność

Wykonawca jest związany ofertą przez okres 30 dni licząc od dnia, w którym upływa dzień na składanie ofert. Płatność nastąpi w terminie 30 dni od dnia zawarcia umowy (od dnia skutecznego dostarczenia faktury, na podstawie podpisanego przez Strony protokołu odbioru przedmiotu zamówienia).

VII. Miejsce, sposób i termin składania ofert:

1. Ofertę cenową z należy przekazać Zamawiającemu na formularzu ofertowym zgodnie ze wzorem stanowiącym Załącznik Nr 1 do dnia **4 grudnia 2024 r. godz. 10:00**: drogą elektroniczną na adres: https://platformazakupowa.pl
2. Kompletna oferta musi zawierać:
a) Formularz oferty;
b) Pełnomocnictwo(a), jeśli dotyczy.
3. Oferta musi zostać sporządzona w języku polskim (dokumenty sporządzone w języku obcym muszą być złożone wraz z tłumaczeniem na język polski, wystarczające jest tłumaczenie Wykonawcy) i złożona w postaci:
a) oryginału dokumentu, w przypadku dostarczenia oferty w formie tradycyjnej, tj. papierowej lub
b) czytelnego skanu podpisanego dokumentu lub

c) elektronicznej, podpisanej: kwalifikowanym podpisem elektronicznym lub podpisem osobistym lub podpisem zaufanym pod rygorem nieważności.
4. Formularz ofertowy musi być podpisany przez osobę/y składającą/ce Ofertę.
5. Do Oferty należy dostarczyć pełnomocnictwo do podpisania oferty, o ile prawo do podpisania oferty nie wynika z innych dokumentów złożonych wraz z ofertą lub ogólnodostępnych baz/ rejestrów. Treść pełnomocnictwa powinna jednoznacznie określać czynności, co do wykonywania, których pełnomocnik jest upoważniony.
6. Oferty złożone po terminie oraz niezgodnie ze sposobem złożenia określonym w zapytaniu nie będą rozpatrywane.

VIII. Warunki udziału w postępowaniu:
Zamawiający nie precyzuje warunków udziału w postępowaniu.

IX. Opis sposobu przygotowania ofert:
Cena oferty musi być kompletna, jednoznaczna i ostateczna. Wykonawca kalkuluje cenę na podstawie niniejszego zapytania ofertowego.
Oferta powinna zostać złożona na formularzu stanowiącym załącznik nr 1 do zaproszenia i co najmniej zawierać:
– Nazwę produktów z podaniem wersji/nazw modułów;
– Nazwa, dane teleadresowe oferenta;
– Wartość oferty w złotych polskich (wartość brutto oraz stawkę podatku VAT);
– Datę sporządzenia oferty.

X. Badanie i ocena ofert:
1. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert, dokumentów lub oświadczeń.
2. Zamawiający poprawia w ofercie oczywiste omyłki pisarskie, oczywiste omyłki rachunkowe z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek i inne omyłki polegające na niezgodności oferty z dokumentacji zamówienia, niepowodujących istotnych zmian w treści oferty.
3. Treść oferty musi odpowiadać treści zapytania ofertowego.
4. Zamawiający odrzuci ofertę, jeżeli:
a) została złożona po terminie składania ofert;
b) jest nieważna na podstawie odrębnych przepisów;
c) jej treść jest niezgodna z warunkami zamówienia;
d) nie została sporządzona lub przekazana w sposób zgodny z wymaganiami technicznymi oraz organizacyjnymi sporządzania lub przekazywania ofert przy użyciu środków komunikacji elektronicznej określonymi przez zamawiającego;
e) zawiera rażąco niską cenę lub koszt w stosunku do przedmiotu zamówienia (w przypadku badania określonej przesłanki)
f) zawiera błędy w obliczeniu ceny lub kosztu;
g) została złożona w warunkach czynu nieuczciwej konkurencji w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji;
h) wykonawca w wyznaczonym terminie zakwestionował poprawienie omyłki polegającej na niezgodności oferty z dokumentami zamówienia, niepowodującej zmiany w treści oferty;
i) wykonawca nie wyraził pisemnej zgody na przedłużenie terminu związania ofertą;
j) w stosunku do Wykonawcy zachodzą przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 w związku z art. 7 ust. 9 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie

przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2023 r. poz. 1497 ze zm.)[1].

XI. Inne uwarunkowania dot. realizacji przedmiotu zamówienia:

1. Osoba uprawniona do kontaktów w sprawie oferty: Jarosław Smyczyński – tel. 730-987-530
2. Zadanie jest przewidziane do realizacji przy współudziale środków zewnętrznych - dofinansowania z „Cyberbezpiecznego Samorządu".
3. Niniejsze postępowanie prowadzone jest na zasadach opartych na wewnętrznych uregulowaniach Zamawiającego. Postępowanie prowadzone jest zgodnie z zasadą konkurencyjności i nie podlega przepisom Prawo zamówień publicznych.
4. Do prowadzonego postępowania nie przysługują Wykonawcom żadne środki ochrony prawnej określone w przepisach ustawy Prawo zamówień publicznych tj. odwołanie, skarga.
5. Zamawiający zastrzega sobie prawo do zmiany zapytania ofertowego przed upływem terminu do składania ofert. Wszelkie zmiany treści zapytania ofertowego oraz wyjaśnienia udzielone na zapytania Wykonawcy stają się integralną częścią zapytania ofertowego i są wiążące dla Wykonawców.
6. Zamawiający zastrzega sobie prawo do unieważnienia niniejszego postępowania w każdym czasie bez podania uzasadnienia, w tym także pozostawienia postępowania bez wyboru oferty.
7. Wykonawcy, których oferty nie zostaną wybrane nie mogą zgłaszać żadnych roszczeń względem Zamawiającego z tytułu otrzymania zapytania ofertowego oraz przygotowania i złożenia oferty na to zapytanie.
8. Zamawiający zastrzega sobie prawo (możliwość) do zamieszczenia na stronie internetowej prowadzonego postępowania informacji o: złożonych ofertach, wynikach postępowania (udzieleniu zamówienia).
9. Wykonawca, którego oferta zostanie wybrana zostanie powiadomiony pisemnie lub telefonicznie o wyborze jego oferty oraz o terminie i miejscu podpisania (zawarcia) umowy (zlecenia). Zamawiający nie określa (nie przewiduje) warunków istotnych zmian umowy zawartej w wyniku przeprowadzonego postępowania o udzielenie zamówienia. Projektowane postanowienia umowy będą uwzględniały następujące warunki:
    a. W wypadku niewykonania (w tym nieterminowego wykonania) lub nienależytego wykonania umowy Wykonawca zobowiązany będzie do zapłaty na rzecz Zamawiającego kary umownej w wysokości 1,50% wartości brutto przedmiotu umowy za każdy rozpoczęty dzień zwłoki, licząc od dnia upływu terminu dostawy określonego w umowie (zleceniu);
    b. Zamawiający ma prawo odstąpienia od umowy z powodu opóźnienia dostawy powyżej 14 dni. Wykonawca zobowiązany jest zapłacić Zamawiającemu karę umowną za

[1] Zgodnie z art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, zwanej dalej „ustawą", z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp wyklucza się:
1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3;
2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593, z późn. zm. 8) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3;
3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120 i 295) jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3.

odstąpienie od umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy, odstąpienie od umowy przez Wykonawcę z przyczyn leżących po jego stronie – w wysokości 20,00% kwoty wynagrodzenia należnego wykonawcy.

c. Wykonawca wyraża zgodę na potrącenie kar umownych z przysługującego mu wynagrodzenia ustalonego w umowie zawartej z Zamawiającym.

10. Jeżeli Wykonawca, którego oferta została wybrana uchyla się od podpisania umowy, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert.

Maria Pałucka

Signature Not Verified
Dokument podpisany przez Maria Pałucka
Data: 2024.11.25 08:26:53 CET

Zastępca Wójta
Gminy Papowo Biskupie