Jeżów, dn. 07.02.2024 r.

Gmina Jeżów
ul. Kwiatowa 1,
95-047 Jeżów

Zaproszenie do składania ofert

Działając w oparciu o art. 2 ust. 1 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tj. Dz. U z 2023 r., poz. 1605 ze zm.) oraz Zarządzenia Wójta Gminy Jeżów Nr 135/2020 z dnia 31 grudnia 2020 r. w sprawie wprowadzenia Regulaminu udzielania zamówień publicznych, których wartość szacunkowa nie przekracza kwoty 130.000 złotych, Zamawiający, Gmina Jeżów zaprasza do składania ofert.

1. Przedmiot zamówienia:

Zakup wraz z dostawą, wdrożeniem i opieką serwisową urządzenia typu UTM w ramach projektu grantowego pn. „Cyberbezpieczny Samorząd" realizowanego w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa".

2. Szczegółowa specyfikacja przedmiotu zamówienia:

L.p.	Parametr	Minimalne wymagania techniczne
1.	Wymagania ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.

2.	Interfejsy:	1. Urządzenie posiada co najmniej 10 portów Gigabit Ethernet RJ-45, w tym minimum: 2 porty WAN, 1 port DMZ, 2. Urządzenie posiada wbudowany port konsoli szeregowej, 3. Urządzenie posiada gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB, 4. Urządzenie pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
3.	Wydajność	1. W zakresie Firewalla obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę, 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B, 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps, 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps, 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps, 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps, 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.
4.	Redundancja, wykrywanie awarii, monitoring	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji, 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych, 3. Monitoring stanu realizowanych połączeń VPN, 4. Urządzenie umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
5.	Funkcje bezpieczeństwa	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection, 2. Kontrola Aplikacji, 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN, 4. Ochrona przed malware, 5. Ochrona przed atakami - Intrusion Prevention System,

		6. Kontrola stron WWW, 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, 8. Zarządzanie pasmem (QoS, Traffic shaping), 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP), 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site, 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3, 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system, 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
6.	Połączenia VPN	1. Urządzenie umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2, • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM), • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site, • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności, • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego, • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat, • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu, • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu, • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth,

		• Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. Urządzenie umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0, • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta, • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
7.	Firewall, polityki	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.

8.	Zarządzanie pasmem	1. Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Urządzenie daje możliwość określania pasma dla poszczególnych aplikacji. 3. Urządzenie pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. Urządzenie zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
9.	Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. Urządzenie chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
10.	Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane,

		uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
11.	Obsługa łączy WAN, routing	W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
12.	Funkcje SD-WAN	1. Urządzenie umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
13.	Kontrola WWW	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

		2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
14.	Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. Urządzenie daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

15.	Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
16.	Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).

		9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
17.	Logowanie	1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
18.	Zasilanie	Urządzenie jest wyposażony w zasilanie AC.
19.	Serwisy i licencje	Do oferowanego urządzenia Wykonawca dostarczy pakiet niezbędnych licencyjny do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy.
20.	Opieka techniczna	Wykonawca zapewni dodatkową opiekę techniczną w ilości minimum 3 godzin/miesiąc przez okres minimum 24 miesięcy, świadczoną w języku polskim. Wykonawca zapewni możliwość realizacji opieki technicznej z użyciem połączeń zdalnych. Możliwość kontaktu z helpdeskiem w godzinach pracy 8h, przez 5 dni w tygodniu. Opieka techniczna ma obejmować m in.: • mailowe lub telefoniczne składanie zleceń zmian w konfiguracji urządzenia, • diagnostyka problemów technicznych, • przeprowadzanie aktualizacji firmware urządzenia, • konfiguracja reguł firewalla zgodnie z wytycznymi Zamawiającego,

		• konfiguracja reguł filtrów Web Filtering (URL Filtering), • konfiguracja sieci, routingu, NAT, uwierzytelniania użytkowników, • konfiguracja reguł filtrów aplikacji, • konfiguracja reguł zarządzania pasmem (QoS), • konfiguracja antywirusa i antyspamu, • konfiguracja połączeń VPN (IPSec, SSL), • konfiguracja VDOM.
21.	Warunki gwarancji	Termin gwarancji na urządzenie zgodny z okresem wykupionych licencji/serwisów. Gwarancja każdorazowo przedłużana na okres wykupionych serwisów/licencji. Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres wymaganej gwarancji.
22	Dodatkowe usługi	Wykonawca przeprowadzi wdrożenie dostarczonego urządzenia do pracy w sieci teleinformatycznej Zamawiającego. Wdrożenie będzie polegało przede wszystkim na migracji konfiguracji/ustawień z obecnie posiadanego przez Zamawiającego urządzenia UTM FortiGate 50e oraz ewentualnych poprawkach/modyfikacjach w konfiguracji nowego urządzenia, zgodnie z wymogami Zamawiającego i „dobrymi praktykami" w zakresie konfiguracji urządzeń typu UTM. Serwisy i licencje dla starego urządzenia UTM Zamawiającego nie będą przedłużane.
23.	Dostawa	Do siedziby Zamawiającego, na koszt Wykonawcy.

3. Informacje podstawowe:

1) Termin realizacji zamówienia: 21 dni od daty podpisania umowy.

2) Każdy z oferentów może złożyć tylko jedną ofertę,

3) Kryterium wyboru oferty: najniższa cena brutto,

Ocena punktowa oferty będzie dokonana według następującego wzoru:

$$\frac{oferowana\ cena\ najniższa\ brutto}{cena\ badanej\ oferty\ brutto} \times 100 \times 100\%$$

Za najkorzystniejszą zostanie uznana oferta, która uzyska największą ilość punktów.

Ocena oferty wyrażona zostanie w punktach, przy czym 1% oznacza 1 pkt.

4) Oferty złożone po terminie nie będą rozpatrywane,

5) W postępowaniu mogą brać udział Wykonawcy, którzy nie podlegają wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2023 r. poz.1497 ze zm.).

6) Zamawiający zgodnie z art. 7 ust. 3 ustawy z dnia 13 kwietnia 2022r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2023r. poz.1497 ze zm.) odrzuci ofertę Wykonawcy, który podlega wykluczeniu na podstawie art.7 ust.1 w/w ustawy. Osoba lub podmiot podlegające wykluczeniu na podstawie art.7 ust.1 w/w ustawy, które w okresie tego wykluczenia ubiegają się o udzielenie zamówienia publicznego podlegają karze pieniężnej w wysokości do 20 000 000 zł, o czym stanowi art.7 ust.6 i 7 powołanej ustawy.

7) Zamawiający zastrzega sobie prawo odwołania postępowania lub jego zamknięcia bez wybrania którejkolwiek ze złożonych ofert.

8) W celu weryfikacji poprawności złożonej oferty Zamawiający może wezwać Oferenta do przedstawienia szczegółowej specyfikacji technicznej oferowanego przedmiotu zamówienia. Termin udzielenia odpowiedzi na wezwanie nie może przekroczyć 2 dni roboczych od dnia wezwania.

4. Informacje dodatkowe:

Osoba ze strony Zamawiającego wyznaczona do kontaktu: Krzysztof Juraś, tel. 46 875 53 71 wewn. 38, e-mail: informatyk@jezow.pl

5. Termin składania ofert:

Prosimy o dostarczenie oferty cenowej do dnia 12.02.2024 r. do godziny 10:00 na adres mailowy: oferty@jezow.pl.

6. Uwagi:

1) Gmina Jeżów zastrzega sobie prawo do odstąpienia od realizacji zamówienia, w przypadku, gdy najkorzystniejsza oferta cenowa przekroczy środki, które zamawiający przeznaczył na realizację w/w zamówienia.

2) Niniejsze zaproszenie do składania ofert nie stanowi żadnego zobowiązania ze strony Gminy Jeżów. Takie zobowiązanie powstaje dopiero z chwilą podpisania umowy z wybranym Wykonawcą.
3) Zamówienie zostanie udzielone Wykonawcy, który zaoferuje najniższą cenę i oferta spełniać będzie wymogi/warunki określone przez Zamawiającego - Gminę Jeżów w niniejszym zaproszeniu do składania ofert.
4) Do oferty należy dołączyć wypełniony i podpisany „Formularz ofertowy" oraz „Oświadczenie dotyczące przesłanek wykluczenia z postępowania".

Signature Not Verified
Dokument podpisany przez Bartłomiej Lipski
Data: 2024.03.07 09:04:58 CET

Sporządził
Krzysztof Juraś
Urząd Gminy w Jeżowie
ul. Kwiatowa 1
95-047 Jeżów
tel. 46 875 53 71 wewn. 38