Ogłoszenie nr 573891-N-2019 z dnia 2019-07-15 r.

Gmina Moszczenica: Dostawa, instalacja i konfiguracja fabrycznie nowego sprzętu IT dla zadania Podniesienie atrakcyjności inwestycyjnej województwa łódzkiego poprzez kompleksowe uzbrojenie Moszczenickich Terenów Inwestycyjnych (MTI)

OGŁOSZENIE O ZAMÓWIENIU - Dostawy

Zamieszczanie ogłoszenia: Zamieszczanie obowiązkowe

Ogłoszenie dotyczy: Zamówienia publicznego

Zamówienie dotyczy projektu lub programu współfinansowanego ze środków Unii Europejskiej

Tak

Nazwa projektu lub programu

Projekt pn.: „Podniesienie atrakcyjności inwestycyjnej województwa łódzkiego poprzez kompleksowe uzbrojenie Moszczenickich Terenów Inwestycyjnych (MTI)" współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach RPO Województwa Łódzkiego na lata 2014-2020, Oś Priorytetowa: II Innowacyjna i konkurencyjna gospodarka, Działanie: II.1 Otoczenie biznesu, Poddziałanie II.1.1 Tereny inwestycyjne.

O zamówienie mogą ubiegać się wyłącznie zakłady pracy chronionej oraz wykonawcy, których działalność, lub działalność ich wyodrębnionych organizacyjnie jednostek, które będą realizowały zamówienie, obejmuje społeczną i zawodową integrację osób będących członkami grup społecznie marginalizowanych

Nie

Należy podać minimalny procentowy wskaźnik zatrudnienia osób należących do jednej lub więcej kategorii, o których mowa w art. 22 ust. 2 ustawy Pzp, nie mniejszy niż 30%, osób zatrudnionych przez zakłady pracy chronionej lub wykonawców albo ich jednostki (w %)

SEKCJA I: ZAMAWIAJĄCY

Postępowanie przeprowadza centralny zamawiający

Nie

Postępowanie przeprowadza podmiot, któremu zamawiający powierzył/powierzyli przeprowadzenie postępowania

Nie

Informacje na temat podmiotu któremu zamawiający powierzył/powierzyli prowadzenie postępowania:

Postępowanie jest przeprowadzane wspólnie przez zamawiających

Nie

Jeżeli tak, należy wymienić zamawiających, którzy wspólnie przeprowadzają postępowanie oraz podać adresy ich siedzib, krajowe numery identyfikacyjne oraz osoby do kontaktów wraz z danymi do kontaktów:

Postępowanie jest przeprowadzane wspólnie z zamawiającymi z innych państw członkowskich Unii Europejskiej

Nie

W przypadku przeprowadzania postępowania wspólnie z zamawiającymi z innych państw członkowskich Unii Europejskiej – mające zastosowanie krajowe prawo zamówień publicznych:

Informacje dodatkowe:

I. 1) NAZWA I ADRES: Gmina Moszczenica, krajowy numer identyfikacyjny 59064794800000, ul. ul. Kosowska 1 , 97-310 Moszczenica, woj. łódzkie, państwo Polska, tel. 446 169 570, e-mail Tomasz.Mikulski@moszczenica.pl, faks 446 169 625.

Adres strony internetowej (URL): http://www.moszczenica.pl

Adres profilu nabywcy:

Adres strony internetowej pod którym można uzyskać dostęp do narzędzi i urządzeń lub formatów plików, które nie są ogólnie dostępne

I. 2) RODZAJ ZAMAWIAJĄCEGO: Administracja samorządowa

I.3) WSPÓLNE UDZIELANIE ZAMÓWIENIA ***(jeżeli dotyczy)*****:**

Podział obowiązków między zamawiającymi w przypadku wspólnego przeprowadzania postępowania, w tym w przypadku wspólnego przeprowadzania postępowania z zamawiającymi z innych państw członkowskich Unii Europejskiej (który z zamawiających jest odpowiedzialny za przeprowadzenie postępowania, czy i w jakim zakresie za przeprowadzenie postępowania odpowiadają pozostali zamawiający, czy zamówienie będzie udzielane przez każdego z zamawiających indywidualnie, czy zamówienie zostanie udzielone w imieniu i na rzecz pozostałych zamawiających):

I.4) KOMUNIKACJA:

Nieograniczony, pełny i bezpośredni dostęp do dokumentów z postępowania można uzyskać pod adresem (URL)

Tak

http://bip.moszczenica.eu/groups/details/1015/dostawy

Adres strony internetowej, na której zamieszczona będzie specyfikacja istotnych warunków zamówienia

Tak

http://bip.moszczenica.eu/groups/details/1015/dostawy

Dostęp do dokumentów z postępowania jest ograniczony - więcej informacji można uzyskać pod adresem

Nie

Oferty lub wnioski o dopuszczenie do udziału w postępowaniu należy przesyłać:

Elektronicznie

Nie

adres

Dopuszczone jest przesłanie ofert lub wniosków o dopuszczenie do udziału w postępowaniu w inny sposób:

Nie

Inny sposób:

Wymagane jest przesłanie ofert lub wniosków o dopuszczenie do udziału w postępowaniu w inny sposób:

Tak

Inny sposób:

pisemnie

Adres:

Urząd Gminy w Moszczenicy, ul. Kosowska 1, 97-310 Moszczenica

Komunikacja elektroniczna wymaga korzystania z narzędzi i urządzeń lub formatów plików, które nie są ogólnie dostępne

Nie

Nieograniczony, pełny, bezpośredni i bezpłatny dostęp do tych narzędzi można uzyskać pod adresem: (URL)

SEKCJA II: PRZEDMIOT ZAMÓWIENIA

II.1) Nazwa nadana zamówieniu przez zamawiającego: Dostawa, instalacja i konfiguracja fabrycznie nowego sprzętu IT dla zadania Podniesienie atrakcyjności inwestycyjnej województwa łódzkiego poprzez kompleksowe uzbrojenie Moszczenickich Terenów Inwestycyjnych (MTI)

Numer referencyjny: INW.271. 25 .2019

Przed wszczęciem postępowania o udzielenie zamówienia przeprowadzono dialog techniczny

Nie

II.2) Rodzaj zamówienia: Dostawy

II.3) Informacja o możliwości składania ofert częściowych

Zamówienie podzielone jest na części:

Nie

Oferty lub wnioski o dopuszczenie do udziału w postępowaniu można składać w odniesieniu do:

Zamawiający zastrzega sobie prawo do udzielenia łącznie następujących części lub grup części:

Maksymalna liczba części zamówienia, na które może zostać udzielone zamówienie jednemu wykonawcy:

II.4) Krótki opis przedmiotu zamówienia *(wielkość, zakres, rodzaj i ilość dostaw, usług lub robót budowlanych lub określenie zapotrzebowania i wymagań)* **a w przypadku partnerstwa innowacyjnego - określenie zapotrzebowania na innowacyjny produkt, usługę lub roboty budowlane:** 1. Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja fabrycznie nowego sprzętu IT w postaci przełączników oraz urządzenia firewall na potrzeby realizacji projektu pn.: Podniesienie atrakcyjności inwestycyjnej województwa łódzkiego poprzez kompleksowe uzbrojenie Moszczenickich Terenów Inwestycyjnych (MTI). 2. Wspólny Słownik Zamówień (CPV): 30230000-0 Sprzęt związany z komputerami 30200000-1 Urządzenia komputerowe 48000000-8 Pakiety oprogramowania i systemy informatyczne

32420000-3 Urządzenia sieciowe 32520000-4 Sprzęt i kable telekomunikacyjne 3.1. Przełączniki rdzeniowe – 2 szt. Elementem dostawy są dwa przełączniki rdzeniowe, optyczne, pracujące w standardzie 10Gb Ethernet, wraz z kompletem kabli umożliwiających połączenie w stos o następujących minimalnych parametrach każdy: Porty przełącznika: minimum 48*10G (SFP+), minimum 6*40G (QSFP+) z możliwością rozszycia każdego portu na 4x10G Stackowanie: możliwość połączenia minimum 4 przełączników w stos za pomocą portów SFP+ lub QSFP+ bez dedykowanego okablowania (wymagane dostarczenie okablowania typu DAC) Matryca przełączająca: 1440 Gb/s Przepustowość pakietów: minimum 1071 Mp/s (dla pakietów 64Kb) Pojemność tablicy MAC: minimum 96k (w trybie standard) / 32k (w trybie routee) / 288k (w trybie bridgee) wpisów Tablica routingu: minimum 8k (w trybie standard) / 128k (w trybie routee) / 8k (w trybie bridgee) wpisów Tablica ARP: minimum 208k (w trybie standard) / 16k (w trybie routee) / 16k (w trybie bridgee) wpisów Pamięć Flash: minimum 8GB Pamięć RAM: minimum 4GB Zasilanie urządzenia: minimum dwa modularne, w pełni redundantne zasilacze 230VAC, maksymalny pobór mocy przełącznika do 305W Chłodzenie urządzenia: aktywne, redundantne, minimum 4 wentylatory Certyfikaty bezpieczeństwa: CE, RoHS Ilość wpisów tablicy ACL: minimum 4k Ilość kolejek sprzętowych dla portów GE: minimum 8 Ilość aktywnych IEEE802.1Q VLAN: minimum 4094 Ruting L3: Ruting statyczny, RIPv1/v2, OSPFv2, RIPng, OSPFv3, BGP4+, Ruting LPM, Ruting PBR dla IPv4/IPv6, DVMRP, PIM-DM, PIM-SM, PIM-SSM, Static multicast route, pojemność tabeli routingu minimum 128k wpisów Obsługa VLAN: IEEE 802.1Q, QinQ, selektywne QinQ, elastyczne QinQ Wsparcie dla zdefiniowanych typów VLANów: MAC VLAN, Voice VLAN, PVLAN, Protocol VLAN, Multicast VLAN, N:1 VLAN Translation Obsługa protokołów IP: IPv6 oraz IPv4 Obsługa spanning tree: IEEE 802.1D STP, IEEE 802.1W RSTP, IEEE 802.1S MSTP, Root guard, BPDU guard, BPDU forwarding, BPDU tunnel Obsługa wirtualizacji: wirtualizacja z możliwością łączenia w stos urządzeń znajdujących się w oddalonych względem siebie lokalizacjach minimum do 50km Agregacja LACP: zgodne z IEEE 802.3ad, minimum 128 grup, minimum 8 portów per grupa, LACP Load Balance Inne funkcje L1 i L2: unicast/broadcast/multicast storm-control, GVRP DDM, UDLD, LLDP, LLDP-MED, Port Mirror, sFlow, Virtual Cable Testing Inne funkcje L3: VRRP, URPF, ECMP, BFD, VxLAN, IEEE VEPA, Trill, VSF Obsługa Openflow: Openflow 1.0 Funkcje QoS: SWRR, SP, WRR, DWRR, SDWRR, WRED, traffic shaping, klasyfikacja ruchu w oparciu o: CoS, ToS, DiffServ DSCP, ACL, port Bezpieczeństwo: Port, MAC based authentication, RADIUS, TACACS+, Guest VLAN, Auto VLAN, DHCP/DHCPv6 snooping, port security, IP source guard, ARP Guard, Local ARP Proxy, ARP binding, Anti ARP/NDP cheat, Anti ARP scan Listy kontroli dostępu: IP ACL, MAC ACL, IP-MAC ACL, time ranged ACL, VLAN based ACL, ACL konfigurowane na porcie lub VLANie Multicast: minimum 8000 grup multicastowych, IGMP v1/v2/v3, IGMP snooping, IGMP snooping fast leave, MLD snooping Zarządzanie: CLI, Web/SSL, Telnet, SSH, IPv4/IPv6 SNMP v1/v2c/v3, SNMP Trap, RMON 1,2,3,9, Dual firmware images/configuration files, 802.3ah Firmware oraz konfiguracja: oprogramowanie przełącznika (firmware) dostępny bez ograniczeń czasowych, przez cały okres cyklu życiowego urządzenia poprzez Internet, wsparcie techniczne producenta lub dystrybutora bez konieczności wykupu dodatkowych usług, możliwość wgrania kilku plików z obrazem lub konfiguracją systemu, możliwość wgrania oprogramowania oraz konfiguracji poprzez TFTP/FTP, Obsługa DHCP: DHCP client/server/relay, DHCPv6 relay/server Rodzaj gwarancji: minimum 36 miesięcy, licząc od protokołu odbioru. Wymagane jest dostarczenie gwarancji producenta obejmującego także wsparcie techniczne na okres 36 miesięcy od podpisania protokołu odbioru. Wsparcie techniczne świadczone musi być telefonicznie w języku polskim. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy. 3.2 Urządzenie firewall – 1 szt. Zamawiający wymaga dostarczenia urządzenia firewall zgodnego z poniższymi wymaganiami: Nr Wymagania minimalne 1. 1 Urządzenie musi być dostarczone jako dedykowane urządzenie typu appliance o wysokości maksymalnej 1U, przystosowane do montażu w szafie Rack 19". Całość sprzętu musi być zarządzana przez jednego producenta. 2. 2 Urządzenie musi być wyposażone w ☐ 4 interfejsy 10/100/1000 Ethernet (RJ45) ☐ 8 interfejsy 1GE SFP 3. 3 Urządzenie musi być wyposażone w twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 200 MB. 4. 4 Urządzenie musi być wyposażone dedykowany port konsoli/zarządzania. Port ten musi być wydzielony co najmniej logicznie i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji. 5. 5 Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Minimum 1 Gbps dla Firewall/kontroli aplikacji Minimum 750 Gbps dla Firewall/IPS/Antywirus/kontroli aplikacji Minimum 8.000 tys. nowych połączeń na sekundę Minimum 100.000 równoległych sesji 6. 6 Urządzenie musi umożliwiać działanie co najmniej w trzech trybach pracy a. rutera (tzn. w warstwie 3 modelu OSI) b. przełącznika (tzn. w warstwie 2 modelu OSI) c. w trybie pasywnego nasłuchu (sniffer) d. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA) 7. 7 Tryb pracy urządzenia musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny kontekst/system/firewall/wirtualna domena, itp.) 8. 8 Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q. Urządzenie musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3. 9. 9 Urządzenie musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa, tak aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk. 10. 10 Urządzenie musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN) 11. 11 Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Wydajność IPsec 400Mbps Minimum 500 tuneli IPSEC VPN Minumum 500 tuneli SSL VPN Remote Access Jeżeli wykorzystanie funkcji VPN (IPSec i SSL) wymaga zakupu dodatkowych licencji należy je przewidzieć w ofercie dla maksymalnej jego wydajności tzn. dla 500 jednoczesnych użytkowników. 12. 12 Urządzenie musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach. a. Polityki definiujące powinny umożliwiać wykorzystanie i. adresów źródłowych ii. adresów docelowych iii. użytkowników iv. numerów portów usług v. kategorie URL b. System musi obsługiwać co najmniej następujące mechanizmy uwierzytelnienia i. RADIUS lub TACACS+ ii. LDAP iii. Kerberos lub SAML 2.0 13. 13 Urządzenie musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej ☐ oznaczania pakietów znacznikami DiffServ ☐ ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego ☐ utworzenia co najmniej 8 klas ruchu sieciowego ☐ kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników ☐ kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP ☐ przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego 14. 14 Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. 15. 15 Urządzenie musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP. 16. 16

Urządzenie powinno mieć możliwość obsługi nie mniej niż 5 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1. Wówczas należy przewidzieć w ofercie trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia oraz odpowiednio większą instalację systemu zarządzania (dotyczy liczby zarządzanych firewalli logicznych). 17. 17 Urządzenie musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu. 18. 18 Urządzenie musi umożliwiać obsługę klastra niezawodnościowego – tworzenia konfiguracji odpornej na awarie dla urządzeń. Urządzenia w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active. 19. 19 Polityka bezpieczeństwa systemu zabezpieczeń musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, kategorie URL, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 1.500 reguł polityki bezpieczeństwa. 20. 20 Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65.535 dostępnych portach tcp i udp. Wydajność kontroli firewalla stanowego i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż wskazano w wymaganiach wydajnościowych Urządzenie musi wykrywać co najmniej 2500 predefiniowanych aplikacji wspieranych przez producenta (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. 21. 21 Urządzenie musi przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM), w których informacja o aplikacji będzie mogła być tylko wykorzystana tylko jako „wartość" w polityce. 22. 22 Urządzenie musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie. 23. 23 Urządzenie musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia. 24. 24 Urządzenie musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku, gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji 25. 25 Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download" 26. 26 Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa. 27. 28 Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH. 28. 29 Rozwiązanie musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o: a) Microsoft Active Directory b) usługi katalogowe LDAP c) serwery Terminal Services 29. 30 Polityka kontroli dostępu urządzenia musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana, nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. 30. 31 Urządzenie musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów, z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. Dopuszcza się zastosowanie innego mechanizmu wbudowanego w urządzenie, który technicznie pozwoli na uzyskanie równoważnej funkcjonalności dotyczącej „śledzenia" logowania użytkowników. 31. 32 Urządzenie musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji. System IPS musi działać w warstwie 7 modelu OSI. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. 32. 33 Urządzenie musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji. Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb. Baza sygnatur AV musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń Moduł AV musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). 33. 34 Urządzenie musi zapewniać ochronę przed atakami typu Spyware– Zamawiający dopuszcza, by odbywało się to poprzez silnik AV lub silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Reguły/silnik anty-spyware musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja ta była uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. 34. 36 Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu botnet na podstawie analizy behawioralnej. 35. 37 Urządzenie musi posiadać funkcjonalność URL Flitering wraz z aktualizacją w okresie gwarancji. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL. Moduł filtrowania stron WWW musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. 36. 38 Zarządzanie urządzeniem musi

odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). 37. 39 System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Urządzenie musi umożliwiać uwierzytelnianie administratorów za pomocą a. bazy lokalnej, b. serwera LDAP, c. RADIUS lub TACACS+ Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS). 38. 40 Urządzenie musi zapewniać interfejs API (JSON, REST, XML lub inny) będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI) 39. 41 Urządzenie musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia. 40. 42 Urządzenie musi zapewniać możliwość zatwierdzania zmian per pojedynczy system/firewall /kontekst wirtualny. Zmiany zatwierdzane w pojedynczym firewallu wirtualnym nie mogą być w jakikolwiek sposób widoczne w innych systemach wirtualnych, w szczególności niedopuszczalne jest aby zatwierdzenie zmian w pojedynczym systemie/kontekście wpływało w jakikolwiek sposób na ciągłość komunikacji/filtrację /reguły/polityki etc. w innych systemach wirtualnych 41. 43 Urządzenie musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG. 42. 45 Urządzenie musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się poprzez analizę heurystyczną Urządzenie musi pozwalać na blokowanie transmisji plików szyfrowanych co najmniej a. Dokumentów office (doc, xls, ppt) b. Plików skompresownaych (zip, rar) Urządzenie musi posiadać funkcję automatycznego pobierania z zewnętrznych systemów adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty 43. 46 Urządzenie musi zapewniać wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie sprzętowym. Urządzenie musi posiadać koncept konfiguracji kandydackiej, którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu w tym. a. Możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami. b. Możliwość blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji Urządzenie musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur aplikacyjnych (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa – funkcja ta musi być wbudowana w firewall i nie może wymagać korzystania z rozwiązań trzecich. Urządzenie musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia. Przywrócenie jednej z poprzednich wersji konfiguracji jako konfiguracji aktywnej nie może powodować konieczności restartu urządzenia 44. 47 W przypadku utraty komunikacji z centralną konsolą zarządzania urządzenie musi pozwalać na ▫ Lokalne zbieranie i analizowanie logów ▫ korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: a. ruchu sieciowym b. aplikacjach c. zagrożeniach d. filtrowaniu stron www ▫ tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. ▫ tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu. Okres gwarancji dla urządzenia firewall wynosi minimum 36 miesięcy. Wymagane jest dostarczenie wsparcia producenta na okres 36 miesięcy od podpisania protokołu odbioru. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie w języku polskim i automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Sposób realizacji zgłoszeń gwarancyjny w trybie 8x5xNBD. 3.3 Usługa wsparcia technicznego: Wykonawca przeprowadzi prace instalacyjne i konfiguracyjne wspólnie z administratorami Zamawiającego w jego siedzibie. W ramach prac Wykonawca przekaże wiedzę dotyczącą realizowanej konfiguracji. Po przeprowadzeniu całości prac Wykonawca zapewni szkolenie dla maksymalnie 3 pracowników Zamawiającego w siedzibie Zamawiającego, które będzie obejmowało co najmniej: • Instalację dostarczonych urządzeń • Konfigurację urządzeń i włączenie ich do sieci Zamawiającego • Weryfikację konfiguracji w środowisku produkcyjnym • Backup i odtworzenie konfiguracji. Zamawiający na przedmiotową usługę wsparcia technicznego przewiduje 100 godzin (zegarowych). 3.4 Miejsce realizacji zamówienia Przedmiot zamówienia zostanie zrealizowany w budynku Moszczenickich Terenów Inwestycyjnych w Moszczenicy przy ul. Dworcowej 16. 3.5 Dokumentacja powykonawcza Wykonawca zobowiązany jest do opracowania i dostarczenia dokumentacji technicznej. Dokumentacja musi zawierać plan konfiguracji, implementacji oraz weryfikacji. Dokumentacja zostanie dostarczona na nośniku fizycznym (płyta CD/DVD) lub w formie elektronicznej na adres email podany przez Zamawiającego. Jeżeli w opisie przedmiotu zamówienia użyto nazw, znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty dostarczane przez konkretnego wykonawcę, ich zastosowanie nie jest obowiązkowe, zamawiający dopuszcza zastosowanie rozwiązań równoważnych, a nazwy zostały podane jedynie w celach informacyjnych dla umożliwienia porównania równoważności.

II.5) Główny kod CPV: 30230000-0

Dodatkowe kody CPV:

Kod CPV
30200000-1
48000000-8
32420000-3
32520000-4

II.6) Całkowita wartość zamówienia *(jeżeli zamawiający podaje informacje o wartości zamówienia)*:

Wartość bez VAT:

Waluta:

(w przypadku umów ramowych lub dynamicznego systemu zakupów – szacunkowa całkowita maksymalna wartość w całym okresie obowiązywania umowy ramowej lub dynamicznego systemu zakupów)

II.7) Czy przewiduje się udzielenie zamówień, o których mowa w art. 67 ust. 1 pkt 6 i 7 lub w art. 134 ust. 6 pkt 3 ustawy Pzp: Nie

Określenie przedmiotu, wielkości lub zakresu oraz warunków na jakich zostaną udzielone zamówienia, o których mowa w art. 67 ust. 1 pkt 6 lub w art. 134 ust. 6 pkt 3 ustawy Pzp:

II.8) Okres, w którym realizowane będzie zamówienie lub okres, na który została zawarta umowa ramowa lub okres, na który został ustanowiony dynamiczny system zakupów:

miesiącach: *lub* **dniach:** 30

lub

data rozpoczęcia: *lub* **zakończenia:**

II.9) Informacje dodatkowe: Przedmiot Zamówienia należy wykonać w terminie: do 30 dni od daty podpisania umowy.

SEKCJA III: INFORMACJE O CHARAKTERZE PRAWNYM, EKONOMICZNYM, FINANSOWYM I TECHNICZNYM

III.1) WARUNKI UDZIAŁU W POSTĘPOWANIU

III.1.1) Kompetencje lub uprawnienia do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów

Określenie warunków: Zgodnie z art. 22 ust. 1 ustawy Zamawiający nie określa warunków udziału w postępowaniu w zakresie kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej.

Informacje dodatkowe

III.1.2) Sytuacja finansowa lub ekonomiczna

Określenie warunków: Zgodnie z art. 22 ust. 1 ustawy Zamawiający nie określa warunków udziału w postępowaniu w zakresie sytuacji ekonomicznej lub finansowej.

Informacje dodatkowe

III.1.3) Zdolność techniczna lub zawodowa

Określenie warunków: Zgodnie z art. 22 ust. 1 ustawy Zamawiający nie określa warunków udziału w postępowaniu w zakresie zdolności technicznej lub zawodowej.

Zamawiający wymaga od wykonawców wskazania w ofercie lub we wniosku o dopuszczenie do udziału w postępowaniu imion i nazwisk osób wykonujących czynności przy realizacji zamówienia wraz z informacją o kwalifikacjach zawodowych lub doświadczeniu tych osób: Nie

Informacje dodatkowe:

III.2) PODSTAWY WYKLUCZENIA

III.2.1) Podstawy wykluczenia określone w art. 24 ust. 1 ustawy Pzp

III.2.2) Zamawiający przewiduje wykluczenie wykonawcy na podstawie art. 24 ust. 5 ustawy Pzp Tak Zamawiający przewiduje następujące fakultatywne podstawy wykluczenia: Tak (podstawa wykluczenia określona w art. 24 ust. 5 pkt 1 ustawy Pzp)

Tak (podstawa wykluczenia określona w art. 24 ust. 5 pkt 2 ustawy Pzp)

Tak (podstawa wykluczenia określona w art. 24 ust. 5 pkt 4 ustawy Pzp)

Tak (podstawa wykluczenia określona w art. 24 ust. 5 pkt 8 ustawy Pzp)

III.3) WYKAZ OŚWIADCZEŃ SKŁADANYCH PRZEZ WYKONAWCĘ W CELU WSTĘPNEGO POTWIERDZENIA, ŻE NIE PODLEGA ON WYKLUCZENIU ORAZ SPEŁNIA WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ SPEŁNIA KRYTERIA SELEKCJI

Oświadczenie o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału w postępowaniu

Tak

Oświadczenie o spełnianiu kryteriów selekcji

Nie

III.4) WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW , SKŁADANYCH PRZEZ WYKONAWCĘ W POSTĘPOWANIU NA WEZWANIE ZAMAWIAJACEGO W CELU POTWIERDZENIA OKOLICZNOŚCI, O KTÓRYCH MOWA W ART. 25 UST. 1 PKT 3 USTAWY PZP:

- zaświadczenia właściwego naczelnika urzędu skarbowego potwierdzającego, że wykonawca nie zalega z opłacaniem podatków, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub innego dokumentu potwierdzającego, że wykonawca zawarł porozumienie z właściwym organem podatkowym w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie,

odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu; - zaświadczenia właściwej terenowej jednostki organizacyjnej Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego albo innego dokumentu potwierdzającego, że wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub innego dokumentu potwierdzającego, że wykonawca zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu; - w celu potwierdzenia braku podstaw wykluczenia wykonawcy z udziału w postępowaniu na podstawie art. 24 ust. 5 pkt 1 ustawy zamawiający będzie weryfikował Wykonawcę na podstawie odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji.

III.5) WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW SKŁADANYCH PRZEZ WYKONAWCĘ W POSTĘPOWANIU NA WEZWANIE ZAMAWIAJACEGO W CELU POTWIERDZENIA OKOLICZNOŚCI, O KTÓRYCH MOWA W ART. 25 UST. 1 PKT 1 USTAWY PZP

III.5.1) W ZAKRESIE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU:

III.5.2) W ZAKRESIE KRYTERIÓW SELEKCJI:

III.6) WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW SKŁADANYCH PRZEZ WYKONAWCĘ W POSTĘPOWANIU NA WEZWANIE ZAMAWIAJACEGO W CELU POTWIERDZENIA OKOLICZNOŚCI, O KTÓRYCH MOWA W ART. 25 UST. 1 PKT 2 USTAWY PZP

W celu potwierdzenia spełniania przez oferowane dostawy wymagań określonych przez Zamawiającego, Zamawiający zażąda od Wykonawcy, którego oferta została najwyżej oceniona złożenia w wyznaczonym terminie (nie krótszym niż 5 dni) aktualnych na dzień złożenia następujących dokumentów: - w celu potwierdzenia, że oferowany sprzęt odpowiada wymaganiom określonym przez zamawiającego należy złożyć opis oferowanego sprzętu sporządzony według złącznika Nr 4 do SIWZ.

III.7) INNE DOKUMENTY NIE WYMIENIONE W pkt III.3) - III.6)

1) Formularz ofertowy – wg. Załącznika nr 1 do SIWZ; 2) Dokumenty, z których wynika upoważnienie osób podpisujących ofertę do reprezentacji wykonawcy, w szczególności pełnomocnictwo (o ile w imieniu wykonawcy działa pełnomocnik) lub inne dokumenty potwierdzające umocowanie, jeśli sposób reprezentacji nie wynika z KRS

SEKCJA IV: PROCEDURA

IV.1) OPIS

IV.1.1) Tryb udzielenia zamówienia: Przetarg nieograniczony

IV.1.2) Zamawiający żąda wniesienia wadium:

Nie

Informacja na temat wadium

IV.1.3) Przewiduje się udzielenie zaliczek na poczet wykonania zamówienia:

Nie

Należy podać informacje na temat udzielania zaliczek:

IV.1.4) Wymaga się złożenia ofert w postaci katalogów elektronicznych lub dołączenia do ofert katalogów elektronicznych:

Nie

Dopuszcza się złożenie ofert w postaci katalogów elektronicznych lub dołączenia do ofert katalogów elektronicznych:

Nie

Informacje dodatkowe:

IV.1.5.) Wymaga się złożenia oferty wariantowej:

Nie

Dopuszcza się złożenie oferty wariantowej

Nie

Złożenie oferty wariantowej dopuszcza się tylko z jednoczesnym złożeniem oferty zasadniczej:

Nie

IV.1.6) Przewidywana liczba wykonawców, którzy zostaną zaproszeni do udziału w postępowaniu

(przetarg ograniczony, negocjacje z ogłoszeniem, dialog konkurencyjny, partnerstwo innowacyjne)

Liczba wykonawców

Przewidywana minimalna liczba wykonawców

Maksymalna liczba wykonawców

Kryteria selekcji wykonawców:

IV.1.7) Informacje na temat umowy ramowej lub dynamicznego systemu zakupów:

Umowa ramowa będzie zawarta:

Czy przewiduje się ograniczenie liczby uczestników umowy ramowej:

Przewidziana maksymalna liczba uczestników umowy ramowej:

Informacje dodatkowe:

Zamówienie obejmuje ustanowienie dynamicznego systemu zakupów:

Adres strony internetowej, na której będą zamieszczone dodatkowe informacje dotyczące dynamicznego systemu zakupów:

Informacje dodatkowe:

W ramach umowy ramowej/dynamicznego systemu zakupów dopuszcza się złożenie ofert w formie katalogów elektronicznych:

Przewiduje się pobranie ze złożonych katalogów elektronicznych informacji potrzebnych do sporządzenia ofert w ramach umowy ramowej/dynamicznego systemu zakupów:

IV.1.8) Aukcja elektroniczna

Przewidziane jest przeprowadzenie aukcji elektronicznej *(przetarg nieograniczony, przetarg ograniczony, negocjacje z ogłoszeniem)* Nie

Należy podać adres strony internetowej, na której aukcja będzie prowadzona:

Należy wskazać elementy, których wartości będą przedmiotem aukcji elektronicznej:

Przewiduje się ograniczenia co do przedstawionych wartości, wynikające z opisu przedmiotu zamówienia:

Należy podać, które informacje zostaną udostępnione wykonawcom w trakcie aukcji elektronicznej oraz jaki będzie termin ich udostępnienia:

Informacje dotyczące przebiegu aukcji elektronicznej:

Jaki jest przewidziany sposób postępowania w toku aukcji elektronicznej i jakie będą warunki, na jakich wykonawcy będą mogli licytować (minimalne wysokości postąpień):

Informacje dotyczące wykorzystywanego sprzętu elektronicznego, rozwiązań i specyfikacji technicznych w zakresie połączeń:

Wymagania dotyczące rejestracji i identyfikacji wykonawców w aukcji elektronicznej:

Informacje o liczbie etapów aukcji elektronicznej i czasie ich trwania:

Czas trwania:

Czy wykonawcy, którzy nie złożyli nowych postąpień, zostaną zakwalifikowani do następnego etapu:

Warunki zamknięcia aukcji elektronicznej:

IV.2) KRYTERIA OCENY OFERT

IV.2.1) Kryteria oceny ofert:

IV.2.2) Kryteria

Kryteria	Znaczenie
Cena	60,00
Okres gwarancji	15,00
Czas dostawy	15,00
Termin płatności faktury	10,00

IV.2.3) Zastosowanie procedury, o której mowa w art. 24aa ust. 1 ustawy Pzp (przetarg nieograniczony)

Nie

IV.3) Negocjacje z ogłoszeniem, dialog konkurencyjny, partnerstwo innowacyjne

IV.3.1) Informacje na temat negocjacji z ogłoszeniem

Minimalne wymagania, które muszą spełniać wszystkie oferty:

Przewidziane jest zastrzeżenie prawa do udzielenia zamówienia na podstawie ofert wstępnych bez przeprowadzenia negocjacji

Przewidziany jest podział negocjacji na etapy w celu ograniczenia liczby ofert:

Należy podać informacje na temat etapów negocjacji (w tym liczbę etapów):

Informacje dodatkowe

IV.3.2) Informacje na temat dialogu konkurencyjnego

Opis potrzeb i wymagań zamawiającego lub informacja o sposobie uzyskania tego opisu:

Informacja o wysokości nagród dla wykonawców, którzy podczas dialogu konkurencyjnego przedstawili rozwiązania stanowiące podstawę do składania ofert, jeżeli zamawiający przewiduje nagrody:

Wstępny harmonogram postępowania:

Podział dialogu na etapy w celu ograniczenia liczby rozwiązań:

Należy podać informacje na temat etapów dialogu:

Informacje dodatkowe:

IV.3.3) Informacje na temat partnerstwa innowacyjnego

Elementy opisu przedmiotu zamówienia definiujące minimalne wymagania, którym muszą odpowiadać wszystkie oferty:

Podział negocjacji na etapy w celu ograniczeniu liczby ofert podlegających negocjacjom poprzez zastosowanie kryteriów oceny ofert wskazanych w specyfikacji istotnych warunków zamówienia:

Informacje dodatkowe:

IV.4) Licytacja elektroniczna

Adres strony internetowej, na której będzie prowadzona licytacja elektroniczna:

Adres strony internetowej, na której jest dostępny opis przedmiotu zamówienia w licytacji elektronicznej:

Wymagania dotyczące rejestracji i identyfikacji wykonawców w licytacji elektronicznej, w tym wymagania techniczne urządzeń informatycznych:

Sposób postępowania w toku licytacji elektronicznej, w tym określenie minimalnych wysokości postąpień:

Informacje o liczbie etapów licytacji elektronicznej i czasie ich trwania:

Czas trwania:

Wykonawcy, którzy nie złożyli nowych postąpień, zostaną zakwalifikowani do następnego etapu:

Termin składania wniosków o dopuszczenie do udziału w licytacji elektronicznej:

Data: godzina:

Termin otwarcia licytacji elektronicznej:

Termin i warunki zamknięcia licytacji elektronicznej:

Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia publicznego, albo ogólne warunki umowy, albo wzór umowy:

Wymagania dotyczące zabezpieczenia należytego wykonania umowy:

Informacje dodatkowe:

IV.5) ZMIANA UMOWY

Przewiduje się istotne zmiany postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru wykonawcy: Tak

Należy wskazać zakres, charakter zmian oraz warunki wprowadzenia zmian:



Zgodnie z art. 144 ustawy Zamawiający przewiduje zmiany zawartej umowy w przypadku m.in. zaistnienia następujących okoliczności: 1) zmiany terminu wykonania zamówienia lub terminów płatności będących następstwem zaistnienia siły wyższej, okoliczności, których nie można było przewidzieć przy podpisywaniu Umowy lub zmiany harmonogramu spływu środków finansujących zamówienie z instytucji finansujących, 2) zmiany powszechnie obowiązujących przepisów prawa, w zakresie mającym wpływ na realizację przedmiotu zamówienia, 3) zmiany w przypadku rezygnacji z części zakresu zamówienia jeżeli będzie to niezbędne dla prawidłowej realizacji przedmiotu umowy, 4) zmiana stawki podatku VAT w trakcie trwania umowy i wynikającej z tego tytułu zmiany wysokości wynagrodzenia określonego w § 7 ust. 1 umowy, 5) gdy wykonanie zamówienia w określonym pierwotnie terminie nie leży w interesie Zamawiającego, 6) zmiana dot. zaoferowanego przez Wykonawcę urządzenia oraz terminu realizacji umowy w przypadku zakończenia produkcji określonych produktów lub wycofanie ich z produkcji lub z obrotu na terytorium RP, 7) zmiana dot. zaoferowanego przez Wykonawcę urządzenia oraz terminu realizacji umowy w przypadku upadłości albo likwidacji producenta, dystrybutora lub gwaranta, 8) zmiana dot. zaoferowanego przez Wykonawcę urządzenia oraz terminu realizacji umowy w przypadku istotnych problemów finansowych, ekonomicznych lub organizacyjnych producenta, dystrybutora lub gwaranta uzasadniających ryzyko, że jego produkty, świadczenia itp. mogą nie zostać należycie wykonane lub nie będą miały odpowiedniej jakości albo wsparcia w przyszłości, 9) zmiana terminu realizacji przedmiotu umowy w przypadku uzasadnionych przyczyn technicznych lub funkcjonalnych powodujących konieczność zmiany sposobu wykonania umowy, 10) zmiana terminu realizacji przedmiotu umowy w przypadku konieczności zmiany terminu wykonania lub odbioru dostawy spowodowanej podjęciem przez Zamawiającego decyzji o przeprowadzeniu przez osobę trzecią kontroli jakości i sposobu prowadzenia dostawy. 11) zmiana terminu realizacji przedmiotu umowy w przypadku uzasadnionych przyczyn niezawinionych przez Wykonawcę po zawiadomieniu w sposób określony w § 2 ust. 1 pkt 7 umowy.

IV.6) INFORMACJE ADMINISTRACYJNE

IV.6.1) Sposób udostępniania informacji o charakterze poufnym *(jeżeli dotyczy):*

Środki służące ochronie informacji o charakterze poufnym

IV.6.2) Termin składania ofert lub wniosków o dopuszczenie do udziału w postępowaniu:

Data: 2019-07-23, godzina: 10:00,

Skrócenie terminu składania wniosków, ze względu na pilną potrzebę udzielenia zamówienia (przetarg nieograniczony, przetarg ograniczony, negocjacje z ogłoszeniem):

Nie

Wskazać powody:

Język lub języki, w jakich mogą być sporządzane oferty lub wnioski o dopuszczenie do udziału w postępowaniu

> Polski

IV.6.3) Termin związania ofertą: do: okres w dniach: 30 (od ostatecznego terminu składania ofert)

IV.6.4) Przewiduje się unieważnienie postępowania o udzielenie zamówienia, w przypadku nieprzyznania środków pochodzących z budżetu Unii Europejskiej oraz niepodlegających zwrotowi środków z pomocy udzielonej przez państwa członkowskie Europejskiego Porozumienia o Wolnym Handlu (EFTA), które miały być przeznaczone na sfinansowanie całości lub części zamówienia: Tak

IV.6.5) Przewiduje się unieważnienie postępowania o udzielenie zamówienia, jeżeli środki służące sfinansowaniu zamówień na badania naukowe lub prace rozwojowe, które zamawiający zamierzał przeznaczyć na sfinansowanie całości lub części zamówienia, nie zostały mu przyznane Nie

IV.6.6) Informacje dodatkowe:

ZAŁĄCZNIK I - INFORMACJE DOTYCZĄCE OFERT CZĘŚCIOWYCH

Z up. WÓJTA GMINY
Krzysztof Jędrzejczyk
SEKRETARZ GMINY