Ogłoszenie o zamówieniu
Dostawy
Zakup i dostawa sprzętu komputerowego wraz z oprogramowaniem dla Urzędu Gminy w Osielsku w ramach projektu pn. Cyfrowa Gmina

SEKCJA I - ZAMAWIAJĄCY

1.1.) Rola zamawiającego

Postępowanie prowadzone jest samodzielnie przez zamawiającego

1.2.) Nazwa zamawiającego: Gmina Osielsko

1.4) Krajowy Numer Identyfikacyjny: REGON 092350688

1.5) Adres zamawiającego

1.5.1.) Ulica: Szosa Gdańska 55A

1.5.2.) Miejscowość: Osielsko

1.5.3.) Kod pocztowy: 86-031

1.5.4.) Województwo: kujawsko-pomorskie

1.5.5.) Kraj: Polska

1.5.6.) Lokalizacja NUTS 3: PL613 - Bydgosko-toruński

1.5.7.) Numer telefonu: 52 324 18 64

1.5.9.) Adres poczty elektronicznej: zampub@osielsko.pl

1.5.10.) Adres strony internetowej zamawiającego: www.bip.osielsko.pl

1.6.) Rodzaj zamawiającego: Zamawiający publiczny - jednostka sektora finansów publicznych - jednostka samorządu terytorialnego

1.7.) Przedmiot działalności zamawiającego: Ogólne usługi publiczne

SEKCJA II – INFORMACJE PODSTAWOWE

2.1.) Ogłoszenie dotyczy:

Zamówienia publicznego

2.2.) Ogłoszenie dotyczy usług społecznych i innych szczególnych usług: Nie

2.3.) Nazwa zamówienia albo umowy ramowej:

Zakup i dostawa sprzętu komputerowego wraz z oprogramowaniem dla Urzędu Gminy w Osielsku w ramach projektu pn. Cyfrowa Gmina

2.4.) Identyfikator postępowania: ocds-148610-a68cd457-6674-11ed-aea3-5a7c432eaced

2.5.) Numer ogłoszenia: 2022/BZP 00444569/01

2.6.) Wersja ogłoszenia: 01

2.7.) Data ogłoszenia: 2022-11-17 14:00

2.8.) Zamówienie albo umowa ramowa zostały ujęte w planie postępowań: Tak

2.9.) Numer planu postępowań w BZP: 2022/BZP 00019844/11/P

2.10.) Identyfikator pozycji planu postępowań:

1.2.3 Zakup sprzętu komputerowego w ramach projektu pn. Cyfrowa Gmina

2.11.) O udzielenie zamówienia mogą ubiegać się wyłącznie wykonawcy, o których mowa w art. 94 ustawy: Nie

2.14.) Czy zamówienie albo umowa ramowa dotyczy projektu lub programu współfinansowanego ze środków Unii Europejskiej: Tak

2.15.) Nazwa projektu lub programu

Program Operacyjny Polska Cyfrowa na lata 2014-2020 Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotyczące realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21-00

2.16.) Tryb udzielenia zamówienia wraz z podstawą prawną

Zamówienie udzielane jest w trybie podstawowym na podstawie: art. 275 pkt 1 ustawy

SEKCJA III – UDOSTĘPNIANIE DOKUMENTÓW ZAMÓWIENIA I KOMUNIKACJA

3.1.) Adres strony internetowej prowadzonego postępowania
www.bip.osielsko.pl

3.2.) Zamawiający zastrzega dostęp do dokumentów zamówienia: Nie

3.4.) Wykonawcy zobowiązani są do składania ofert, wniosków o dopuszczenie do udziału w postępowaniu, oświadczeń oraz innych dokumentów wyłącznie przy użyciu środków komunikacji elektronicznej: Tak

3.5.) Informacje o środkach komunikacji elektronicznej, przy użyciu których zamawiający będzie komunikował się z wykonawcami - adres strony internetowej: www.bip.osielsko.pl

3.6.) Wymagania techniczne i organizacyjne dotyczące korespondencji elektronicznej: Komunikacja między Zamawiającym a Wykonawcami, odbywa się przy użyciu środków komunikacji elektronicznej - miniPortalu https://miniportal.uzp.gov.pl/, ePUAPu https://epuap.gov.pl/wps/portal lub poczty elektronicznej, w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. Zamawiający zastrzega sobie możliwość komunikowania się z Wykonawcami za pomocą poczty elektronicznej, na adres podany przez nich w złożonej ofercie. adres e-mail: zampub@osielsko.pl lub sekretariat@osielsko.pl
Zamawiający dopuszcza również możliwość składania dokumentów elektronicznych (z wyłączeniem oferty) za pomocą poczty elektronicznej, adres e-mail: zampub@osielsko.pl Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego, musi posiadać konto na ePUAP. Wykonawca posiadający konto na ePUAP ma dostęp do formularzy: złożenia, zmiany, wycofania oferty lub wniosku oraz do formularza do komunikacji. Wymagania techniczne i organizacyjne wysyłania i odbierania dokumentów elektronicznych, elektronicznych kopii dokumentów i oświadczeń oraz informacji przekazywanych przy ich użyciu opisane zostały w Regulaminie korzystania z miniPortalu oraz Regulaminu ePUAP. Maksymalny rozmiar plików przesyłanych za pośrednictwem dedykowanych formularzy do złożenia, zmiany, wycofania oferty lub wniosku oraz do komunikacji wynosi 150 MB. Wykonawca składa ofertę za pośrednictwem Formularza do złożenia, zmiany, wycofania oferty lub wniosku dostępnego na ePUAP i udostępnionego również na miniPotralu. Formularz do zaszyfrowania oferty przez Wykonawcę jest dostępny dla wykonawców na miniPortalu, w szczegółach danego postępowania. W formularzu oferty/wniosku Wykonawca zobowiązany jest podać adres skrzynki ePUAP, na którym prowadzona będzie korespondencja związana z postępowaniem.
Zaleca się sporządzenie przekazywanych oświadczeń lub dokumentów w formacie .pdf, a także – w przypadku opatrywania ich kwalifikowanym podpisem elektronicznym – złożenie podpisu w formacie PAdES. W przypadku podpisywania oświadczeń lub dokumentów sporządzonych w formacie innym niż .pdf – w przypadku opatrywania ich kwalifikowanym podpisem elektronicznym – zaleca się zastosowanie kwalifikowanego podpisu elektronicznego w formacie XAdES w wariancie wewnętrznym. W przypadku użycia kwalifikowanego podpisu elektronicznego w formacie XAdES w wariancie zewnętrznym, należy pamiętać aby przekazać zarówno podpisywane oświadczenie lub dokument oraz plik podpisu zewnętrznego.

Opatrzenie oświadczeń lub dokumentów podpisem zaufanym możliwe jest w serwisie gov.pl pod adresem: https://www.gov.pl/web/gov/podpisz-dokument-elektronicznie-wykorzystaj podpis-zaufany . Aby opatrzyć oświadczenia lub dokumenty podpisem zaufanym należy posiadać profil zaufany ePUAP. Szczegóły dotyczące zakładania profilu zaufanego znajdują się na stronie serwisu gov.pl pod adresem: https://www.gov.pl/web/gov/zaloz-profil-zaufany

Opatrzenie oświadczeń lub dokumentów podpisem osobistym wymaga posiadania dowodu osobistego z certyfikatem podpisu osobistego: „e-dowodu" oraz specjalistycznego czytnika. Szczegóły dotyczące podpisu osobistego oraz e-dowodu znajdują się w serwisie gov.pl pod adresem: https://www.gov.pl/web/e-dowod/podpis-osobisty

3.8.) Zamawiający wymaga sporządzenia i przedstawienia ofert przy użyciu narzędzi elektronicznego modelowania danych budowlanych lub innych podobnych narzędzi, które nie są ogólnie dostępne: Nie

3.12.) Oferta - katalog elektroniczny: Nie dotyczy

3.14.) Języki, w jakich mogą być sporządzane dokumenty składane w postępowaniu:

polski

3.15.) RODO (obowiązek informacyjny): Zgodnie z art. 13 ust. 1 - 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE Dz. Urz. UE L 119 z 04.05.2016, str. 1 z późn. zm.), dalej „RODO", informuję, że:
1. Administratorem Pani/Pana danych osobowych jest Gmina Osielsko ul. Szosa Gdańska 55A, 86-031 Osielsko tel. 52 324-18-00;
2. Inspektorem ochrony danych osobowych w Urzędzie Gminy Osielsko jest Pani Violetta Dąbrowska, wybory@osielsko.pl, tel. 52 324-18-80;
3. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o

udzielenie zamówienia publicznego na „Zakup i dostawę sprzętu komputerowego wraz z oprogramowaniem o dla Urzędu Gminy w Osielsku w ramach projektu pn. Cyfrowa Gmina”, znak: IiZP.271.D.5.2022 prowadzonym w trybie podstawowym;
4. Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t. j. Dz. U. z 2022 r., poz. 1710), dalej „ustawa Pzp”;
5. Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ustawy Pzp, przez okres 4 lat od zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
6. Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
7. W odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO;
8. Posiada Pani/Pan:
- na podstawie art. 15 RODO prawo dostępu do danych osobowych dotyczących Pani/Pana;
- na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych;
- na podstawie art. 18 RODO prawo do żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;
- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych dotyczących Pani/Pana narusza przepisy RODO;
9. nie przysługuje Pani/Panu:
- w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
- prawo do przenoszenia danych osobowych, o których mowa w art. 20 RODO;
- na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

SEKCJA IV – PRZEDMIOT ZAMÓWIENIA

4.1.) Informacje ogólne odnoszące się do przedmiotu zamówienia.

4.1.1.) Przed wszczęciem postępowania przeprowadzono konsultacje rynkowe: Nie

4.1.2.) Numer referencyjny: IiZP.271.D.5.2022

4.1.3.) Rodzaj zamówienia: Dostawy

4.1.4.) Zamawiający udziela zamówienia w częściach, z których każda stanowi przedmiot odrębnego postępowania: Nie

4.1.8.) Możliwe jest składanie ofert częściowych: Tak

4.1.9.) Liczba części: 3

4.1.10.) Ofertę można składać na wszystkie części

4.1.11.) Zamawiający ogranicza liczbę części zamówienia, którą można udzielić jednemu wykonawcy: Nie

4.1.13.) Zamawiający uwzględnia aspekty społeczne, środowiskowe lub etykiety w opisie przedmiotu zamówienia: Nie

4.2. Informacje szczegółowe odnoszące się do przedmiotu zamówienia:

Część 1

4.2.2.) Krótki opis przedmiotu zamówienia

Przedmiotem zamówienia jest zakup i dostawa sprzętu komputerowego wraz z oprogramowaniem dla Urzędu Gminy w Osielsku w ramach projektu pn. Cyfrowa Gmina, według poniższych specyfikacji:

Część 1: Zakup macierzy dyskowej

Nazwa parametru Minimalna wartość parametru
Obudowa Do instalacji w standardowej szafie RACK 19”, macierz musi zajmować maksymalnie 2U i pozwalać na instalacje 12 dysków 3.5”.
Kontrolery Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów 25Gb iSCSI w Standardzie Sfp+/SFP28
Dołączone minimum dwa transmitery optyczne SFP+ 10Gb SR
Cache 16GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, podtrzymywana bateryjnie przez min. 72h w razie awarii.
Dyski Zainstalowane:
5 dysków Hot-Plug o pojemności 4TB SAS 12Gbps 3,5”,

Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do łącznie minimum 264 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki.

Oprogramowanie/
Funkcjonalności Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5.
Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN'ów oraz 1024 kopii migawkowych na całą macierz.
Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między rożnymi typami dysków.
Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 4TB poprzez dyski SSD.
Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji.
Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym.
Wsparcie dla systemów operacyjnych Windows Server 2022, Windows Server 2019, Windows Server 2016, Red Hat Enterprise Linux (RHEL), SLES, Vmware ESXi, Citrix XenServer
Bezpieczeństwo Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne.
Warunki gwarancji dla macierzy 3 lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.

Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.

Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając,że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygasnięcia gawarancji macierzy.
Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu.
Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części I transportu.
W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).
Dokumentacja użytkownika Zamawiający wymaga dokumentacji w języku polskim lub angielskim
Certyfikaty Macierz musi być wyprodukowany zgodnie z normą ISO 9001:2015.

4.2.6.) Główny kod CPV: 30233000-1 - Urządzenia do przechowywania i odczytu danych

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: 28 dni

4.2.11.) Zamawiający przewiduje wznowienia: Nie

4.2.13.) Zamawiający przewiduje udzielenie dotychczasowemu wykonawcy zamówień na podobne usługi lub roboty budowlane: Nie

4.3.) Kryteria oceny ofert:

4.3.1.) Sposób oceny ofert: Najkorzystniejszą ofertą będzie oferta, która uzyska największą sumę punktów w kryterium „cena" i kryterium " Termin realizacji dostawy".

4.3.2.) Sposób określania wagi kryteriów oceny ofert: Procentowo

4.3.3.) Stosowane kryteria oceny ofert: Kryterium ceny oraz kryteria jakościowe

Kryterium 1

4.3.5.) Nazwa kryterium: Cena

4.3.6.) Waga: 60

Kryterium 2

4.3.4.) Rodzaj kryterium: inne.

4.3.5.) Nazwa kryterium: termin realizacji dostawy

4.3.6.) Waga: 40

4.3.10.) Zamawiający określa aspekty społeczne, środowiskowe lub innowacyjne, żąda etykiet lub stosuje rachunek kosztów cyklu życia w odniesieniu do kryterium oceny ofert: Nie

Część 2

4.2.2.) Krótki opis przedmiotu zamówienia

Przedmiotem zamówienia jest zakup i dostawa sprzętu komputerowego wraz z oprogramowaniem dla Urzędu Gminy w Osielsku w ramach projektu pn. Cyfrowa Gmina, według poniższych specyfikacji:
Część 2: Zakup urządzenia UTM

Wymagania Ogólne
System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
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.
Redundancja, monitoring i wykrywanie awarii
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. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie:
1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
• 8 portami Gigabit Ethernet RJ-45.
• 2 gniazdami SFP 1 Gbps.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System realizujący funkcję Firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności minimum 128 GB.
5. System jest wyposażony w zasilanie AC.
Parametry wydajnościowe:
1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 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 900 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.
Funkcje Systemu 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).
Polityki, Firewall
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.
Połączenia VPN
1. System 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. System 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.
Routing i obsługa łączy WAN
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.
Funkcje SD-WAN
1. System 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).
Zarządzanie pasmem
1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
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).
ciąg dalszy zgodnie z SWZ cz. II str. 7 -10

4.2.6.) Główny kod CPV: 32420000-3 - Urządzenia sieciowe

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: 28 dni

4.2.11.) Zamawiający przewiduje wznowienia: Nie

4.2.13.) Zamawiający przewiduje udzielenie dotychczasowemu wykonawcy zamówień na podobne usługi lub roboty budowlane: Nie

4.3.) Kryteria oceny ofert:

4.3.1.) Sposób oceny ofert: Najkorzystniejszą ofertą będzie oferta, która uzyska największą sumę punktów w kryterium „cena" i kryterium “ Termin realizacji dostawy”.

4.3.2.) Sposób określania wagi kryteriów oceny ofert: Procentowo

4.3.3.) Stosowane kryteria oceny ofert: Kryterium ceny oraz kryteria jakościowe

Kryterium 1

4.3.5.) Nazwa kryterium: Cena

4.3.6.) Waga: 60

Kryterium 2

4.3.4.) Rodzaj kryterium: inne.

4.3.5.) Nazwa kryterium: termin realizacji dostawy

4.3.6.) Waga: 40

4.3.10.) Zamawiający określa aspekty społeczne, środowiskowe lub innowacyjne, żąda etykiet lub stosuje rachunek kosztów cyklu życia w odniesieniu do kryterium oceny ofert: Nie

Część 3

4.2.2.) Krótki opis przedmiotu zamówienia

Przedmiotem zamówienia jest zakup i dostawa sprzętu komputerowego wraz z oprogramowaniem dla Urzędu Gminy w Osielsku w ramach projektu pn. Cyfrowa Gmina, według poniższych specyfikacji:

Część 3: Zakup i dostawa oprogramowania z licencją na Backup na 6 serwerów virtrualnych oraz 5 stacji roboczych

Wymagania do oprogramowania do Backupu dla 5 komputerów, 6 wirtualnych serwerów, licencje bezterminowe
1. Pełne wsparcie dla systemów rodziny Microsoft Windows Server: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Storage Server 2012 R2 Essentials, Windows Server 2008 R2 Foundation, Windows Server 2008 Foundation z SP2 lub wyższy, Windows Server 2003, Windows Server 2003 R2, Windows 2000 Server/Advanced Server (SP4 lub nowszy),
2. Pełne wsparcie dla systemów rodziny Windows Small Business Server: Windows Server 2012 R2 (Essentials, Foundation), Windows Server 2012 (Essentials, Foundation), Windows Small Business Server 2011, Windows Small Business Server 2008 (Standard i Premium), Windows Server 2008 R2 Foundation, Windows Small Business Server 2003 i R2
3. Pełne wsparcie dla środowisk wirtualnych: VMware Workstation, VMware ESX/ESXi, Microsoft Hyper-V, Microsoft Virtual PC, Microsoft Virtual Server, Oracle VirtualBox, Citrix XenServer, Linux KVM, ProxMox, Red Hat Enterprise Virtualization

(RHEV), Stratos everRun.
4. Wsparcie dla 32 i 64-bitowych systemów Microsoft.
5. Wsparcie systemów plików: FAT16, FAT16X, FAT32, FAT32X, NTFS.
6. Wsparcie dla dysków z tablicą partycji MBR oraz GPT
7. Pełne wsparcie dla systemów Ubuntu 14.04, 16.04, 18.04, CentOS 6, CentOS 7, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Oracle Linux (wszystkie systemy 64-bitowe).
8. Wsparcie systemów plików: ext2, ext3, ext4, XFS.
9. Program i wsparcie techniczne dostępne w języku polskim
10. Wsparcie dla 32 i 64-bitowych systemów Microsoft: Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10.

Tworzenie kopii zapasowych (backupu)
1. Backup obejmuje kopie całego systemu operacyjnego wraz z konfiguracją oraz zainstalowanymi aplikacjami i plikami.
2. Program umożliwia skonfigurowanie różnych schematów wykonywania backupu: w trybie pełnym, backupy przyrostowe lub tryb mieszany. Harmonogram przyrostowy powinien umozliwiać backup z częstotliwością min. co 15 minut.
3. Istnieje możliwość wykonywania backupów pełnych i przyrostowych na dyski lokalne, dyski sieciowe, SAN, NAS, dyski USB, Firewire.
4. Program wykonuje kopie zapasowe (backupy) na poziomie sektorów czyli backup przyrostowy zawiera tylko zmienione sektory na dysku a nie np. całe pliki.
5. Program nie wymaga oddzielnego serwera zarządzającego backupem, a harmonogram zadań tworzenia backupów dla danej maszyny jest przechowywany bezpośrednio na tej maszynie.
6. Możliwe jest tworzenie kopii zapasowej w automatycznym trybie hot backupu (bez korzystania ze skryptów zamykających i uruchamiających bazy czy programy). Hot backup powinien pozwalać na backup systemu, aplikacji i baz danych takich MS SQL, MS Exchange, Active Directory, Share Point, Oracle od wersji 11g.
7. Do wykonywania kopii zapasowej wykorzystywana jest technologia Microsoft VSS oraz certyfikowany sterownik Microsoftu.
8. Program umożliwia wykonywanie kopii zapasowej dysku bez konieczności uruchamiania systemu operacyjnego za pomocą bootowalnej płyty lub pendrive’a z systemem i oprogramowaniem dostarczanym przez producenta rozwiązania backupowego.
9. Rozwiązanie pozwala na okresową weryfikacje, konsolidację oraz retencję łańcucha backupu przyrostowego z możliwością konfiguracji po jakim czasie mają się one wykonać.
10. Rozwiązanie musi umożliwiać tworzenie backupu przez łącze 3G i WiFi.
11. Podczas tworzenia kopii zapasowej program generuje plik sumy kontrolnej (md5) dla pliku backupu w celu kontroli plików backupu.
12. Program posiada narzędzie pozwalające na automatyczną weryfikację tworzonych plików backupu za pomocą okresowego uruchamiania backupowanego systemu operacyjnego w maszynie wirtualnej, oraz wysłanie zrzutu ekranu z tak uruchomionego systemu do administratora za pomocą wiadomości email.
13. Program umożliwia konwersje kopii zapasowej do plików dysków maszyn wirtualnych w formacie VHD, VMDK, VHDX.
14. Program umożliwia replikację wykonanych plików kopii zapasowych na dyski lokalnie, dyski sieciowe lub do lokalizacji zdalnych na serwer FTP.

Przywracanie z kopii zapasowych
15. Możliwość przywrócenia backupu całego obrazu dysku/partycji na takim samym sprzęcie, jak ten który był backupowany jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników do nowego sprzętu lub możliwość dodania sterowników przez użytkownika. Komputer powinien zostać uruchomiony z bootowalnej płyty CD lub pendrive’a, z którego bezpośrednio zostaje uruchomiony proces odzyskiwania obrazu dysku z backupu.
16. Program pozwala na dowolne odtwarzanie maszyn fizycznych na inną fizyczną lub do maszyny wirtualnej, oraz z maszyny wirtualnej do innej maszyny wirtualnej lub na fizyczną.
17. Bez względu na rozmiar backupu, program umożliwia automatyczne uruchomienie systemu z backupu jako maszyny wirtualnej w środowiskach VirtualBox, VMware vSphere lub Hyper-V bez konieczności wcześniejszej konwersji pliku backupu do postaci wirtualnej.
18. Program umożliwia zamontowanie pliku backupu jako dysku wirtualnego w trybie odczyt/zapis lub tylko do odczytu. Tak podłączony dysk logiczny umożliwia przeglądanie, wyszukiwanie i odzyskiwanie plików, folderów a także modyfikowanie zawartości.
19. Podczas przywracania obrazu dysku/partycji z kopii zapasowej, program umożliwia: uaktywnienie wybranej partycji, przywrócenia sektora MBR, przywrócenie sygnatur dysku, przywrócenie ukrytych ścieżek na dysku, dezaktywację licencji systemu Windows.
20. Program pozwala na zdefiniowanie procesu tworzenia kolejnych backupów przyrostowych, które w sposób automatyczny będą odtwarzane po określonym przez administratora czasie na innej maszynie fizycznej lub wirtualnej (VMDK, VHD, VHDX). Musi istnieć możliwość zdefiniowania opóźnienia z jakim kopie przyrostowe będą przenoszone na nowy wolumin w zakresie od 1 godziny do 30 dni.

Zdalne zarządzanie
21. Program musi umożliwiać pełną konfigurację i pełne zarządzanie zadaniami wykonywania kopii zapasowej na innych komputerach w sieci lokalnej, w zakresie identycznym jak z lokalnej konsoli administracyjnej.
22. Musi być dostępne narzędzie dające możliwość tworzenia zadań backupu za pomocą polityk dla grup stacji z poziomu

konsoli webowej.
23. Konsola webowa musi umożliwiać instalację oraz aktualizację zdalną oprogramowania na punktach końcowych.
24. Konsola webowa musi umożliwiać podgląd dzienników zdarzeń na stacjach końcowych.
25. Program musi umożliwiać wysłanie powiadomień w postaci wiadomości e-mail gdy: zadanie backupu zakończyło się niepowodzeniem, po zakończeniu zadania tworzenia backupu, oraz podsumowanie aktywności dziennej, tygodniowej i miesięcznej.
26. Musi istnieć możliwość pobrania ze strony producenta konsoli zarządzającej w postaci pliku ISO.

4.2.6.) Główny kod CPV: 72268000-1 - Usługi dostawy oprogramowania

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: 28 dni

4.2.11.) Zamawiający przewiduje wznowienia: Nie

4.2.13.) Zamawiający przewiduje udzielenie dotychczasowemu wykonawcy zamówień na podobne usługi lub roboty budowlane: Nie

4.3.) Kryteria oceny ofert:

4.3.1.) Sposób oceny ofert: Najkorzystniejszą ofertą będzie oferta, która uzyska największą sumę punktów w kryterium „cena" i kryterium “ Termin realizacji dostawy”.

4.3.2.) Sposób określania wagi kryteriów oceny ofert: Procentowo

4.3.3.) Stosowane kryteria oceny ofert: Kryterium ceny oraz kryteria jakościowe

Kryterium 1

4.3.5.) Nazwa kryterium: Cena

4.3.6.) Waga: 60

Kryterium 2

4.3.4.) Rodzaj kryterium: inne.

4.3.5.) Nazwa kryterium: termin realizacji dostawy

4.3.6.) Waga: 40

4.3.10.) Zamawiający określa aspekty społeczne, środowiskowe lub innowacyjne, żąda etykiet lub stosuje rachunek kosztów cyklu życia w odniesieniu do kryterium oceny ofert: Nie

SEKCJA V - KWALIFIKACJA WYKONAWCÓW

5.1.) Zamawiający przewiduje fakultatywne podstawy wykluczenia: Tak

5.2.) Fakultatywne podstawy wykluczenia:

Art. 109 ust. 1 pkt 1

Art. 109 ust. 1 pkt 2 lit a

Art. 109 ust. 1 pkt 2 lit b

Art. 109 ust. 1 pkt 2 lit c

Art. 109 ust. 1 pkt 4

Art. 109 ust. 1 pkt 5

Art. 109 ust. 1 pkt 8

5.3.) Warunki udziału w postępowaniu: Nie

5.5.) Zamawiający wymaga złożenia oświadczenia, o którym mowa w art.125 ust. 1 ustawy: Tak

5.6.) Wykaz podmiotowych środków dowodowych na potwierdzenie niepodlegania wykluczeniu: 1. W celu potwierdzenia braku podstaw wykluczenia Wykonawcy z udziału w postępowaniu zamawiający żąda następujących podmiotowych środków dowodowych:
1) informacja z Krajowego Rejestru Karnego w zakresie:
a) art. 108 ust. 1 pkt 1 i 2 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych, zwanej dalej "ustawą",
b) art. 108 ust. 1 pkt 4 ustawy, dotyczącej orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka karnego,

c) art. 109 ust. 1 pkt 2 lit. a ustawy,
d) art. 109 ust. 1 pkt 2 lit. b ustawy, dotyczącej ukarania za wykroczenie, za które wymierzono karę aresztu,
- sporządzonej nie wcześniej niż 6 miesięcy przed jej złożeniem;
2) zaświadczenia właściwego naczelnika urzędu skarbowego potwierdzającego, że wykonawca nie zalega z opłacaniem podatków i opłat, w zakresie art. 109 ust. 1 pkt 1 ustawy, wystawionego nie wcześniej niż 3 miesiące przed jego złożeniem, a w przypadku zalegania z opłacaniem podatków lub opłat wraz z zaświadczeniem zamawiający żąda złożenia dokumentów potwierdzających, że odpowiednio przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert wykonawca dokonał płatności należnych podatków lub opłat wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłat tych należności;
3) zaświadczenia albo innego dokumentu właściwej terenowej jednostki organizacyjnej Zakładu Ubezpieczeń Społecznych lub właściwego oddziału regionalnego lub właściwej placówki terenowej Kasy Rolniczego Ubezpieczenia Społecznego potwierdzającego, że wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne i zdrowotne, w zakresie art. 109 ust. 1 pkt 1 ustawy, wystawionego nie wcześniej niż 3 miesiące przed jego złożeniem, a w przypadku zalegania z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne wraz z zaświadczeniem albo innym dokumentem zamawiający żąda złożenia dokumentów potwierdzających, że odpowiednio przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert wykonawca dokonał płatności należnych składek na ubezpieczenia społeczne lub zdrowotne wraz odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłat tych należności;
4) odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 ustawy, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;
5) Oświadczenia własne Wykonawcy w zakresie wskazanym w SWZ część IV ust. 4.2 pkt 1,4,5,6,7 (art. 109 ust. 1 pkt.1, 5, 8, 9 i 10 ustawy Pzp).

2. Zamawiający żąda od wykonawcy, który polega na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 118 Pzp, przedstawienia w odniesieniu do tych podmiotów dokumentów wymienionych w Części VII ust. 1 pkt 1-5 SWZ

3. W przypadku wykonawców składających wspólnie ofertę dokumenty, o których mowa w ust.1 składają wszyscy wykonawcy.

SEKCJA VI - WARUNKI ZAMÓWIENIA

6.1.) Zamawiający wymaga albo dopuszcza oferty wariantowe: Nie

6.3.) Zamawiający przewiduje aukcję elektroniczną: Nie

6.4.) Zamawiający wymaga wadium: Nie

6.5.) Zamawiający wymaga zabezpieczenia należytego wykonania umowy: Nie

6.6.) Wymagania dotyczące składania oferty przez wykonawców wspólnie ubiegających się o udzielenie zamówienia:
W przypadku oferty składanej wspólnie przez kilku Wykonawców ubiegających się o udzielenie zamówienia, ocena warunków określonych w pkt. 2.1. SWZ będzie dokonana łącznie w stosunku do Wykonawców ubiegających się wspólnie o udzielenie zamówienia. Każdy z warunków może być spełniony wspólnie przez jednego, kilku lub wszystkich wykonawców łącznie.
W stosunku do żadnego z wykonawców składających ofertę wspólną nie mogą zajść przesłanki wykluczenia określone w art. 108 ust. 1 Pzp i art. 109 ust. 1 Pzp (w zakresie określonym przez Zamawiającego)
Wykonawcy wspólnie ubiegający się o udzielenie zamówienia ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
Przepisy dotyczące Wykonawcy stosuje się odpowiednio do wykonawców wspólnie ubiegających się o udzielenie zamówienia.
Jeżeli oferta wykonawców wspólnie ubiegających się o udzielenie zamówienia zostanie wybrana, Zamawiający będzie żądać przed zawarciem umowy w sprawie zamówienia publicznego, umowy regulującej współpracę tych wykonawców.

6.7.) Zamawiający przewiduje unieważnienie postępowania, jeśli środki publiczne, które zamierzał przeznaczyć na sfinansowanie całości lub części zamówienia nie zostały przyznane: Nie

SEKCJA VII - PROJEKTOWANE POSTANOWIENIA UMOWY

7.1.) Zamawiający przewiduje udzielenia zaliczek: Nie

7.3.) Zamawiający przewiduje zmiany umowy: Tak

7.4.) Rodzaj i zakres zmian umowy oraz warunki ich wprowadzenia:
1. Zmiana postanowień zawartej umowy może nastąpić za zgodą obu stron wyrażoną na piśmie pod rygorem nieważności takiej zmiany.
2. Zamawiający przewiduje możliwość zmiany umowy, w formie aneksu, gdy wystąpią okoliczności, o których mowa w art. art. 455 ust. 1 pkt 1-4 oraz ust. 2 ustawy Pzp.
3. Zamawiający przewiduje również możliwość zmiany umowy:
a) w zakresie przedłużenia terminu realizacji umowy, spowodowanym siłą wyższą bądź innymi przyczynami natury obiektywnej związanymi z obowiązkiem uzyskania odpowiednich zezwoleń lub decyzji, których przy wykazaniu należytej

staranności po stronie wykonawcy, nie udało się uzyskać w terminie.
b) w zakresie podwykonawstwa
c) zmiany stawki podatku od towarów i usług oraz podatku akcyzowego, w związku ze zmianą obowiązujących przepisów w tym zakresie.
4. Zamawiający przewiduje możliwość zmiany umowy w przypadku, gdy nastąpi zmiana powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację przedmiotu umowy.
5. Niedopuszczalna jest jednak pod rygorem nieważności zmiana postanowień zawartej umowy oraz wprowadzenie nowych postanowień do umowy niekorzystnych dla Zamawiającego, jeżeli przy ich uwzględnieniu należałoby zmienić treść oferty, na podstawie, której dokonano wyboru Wykonawcy, chyba że konieczność wprowadzonych zmian wynika z okoliczności, których nie można było przewidzieć w chwili zawarcia umowy.

7.5.) Zamawiający uwzględnił aspekty społeczne, środowiskowe, innowacyjne lub etykiety związane z realizacją zamówienia: Nie

SEKCJA VIII – PROCEDURA

8.1.) Termin składania ofert: 2022-11-25 10:00

8.2.) Miejsce składania ofert: Wykonawca składa ofertę za pośrednictwem Formularza do złożenia, zmiany, wycofania oferty lub wniosku dostępnego na ePUAP i udostępnionego również na miniPotralu. Formularz do zaszyfrowania oferty przez Wykonawcę jest dostępny dla wykonawców na miniPortalu, w szczegółach danego postępowania.

8.3.) Termin otwarcia ofert: 2022-11-25 11:00

8.4.) Termin związania ofertą: do 2022-12-24

SEKCJA IX – POZOSTAŁE INFORMACJE

Zamawiający informuje, że na podstawie 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 (Dz. U. z 2022 r. poz. 835) 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 ustawy;
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 i 655) 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 ustawy;
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 2021 r. poz. 217, 2105 i 2106), 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 ustawy.
Powyższe wykluczenie następować będzie na okres trwania ww. okoliczności. W przypadku wykonawcy lub uczestnika konkursu wykluczonego na podstawie art. 7 ust. 1 ustawy, zamawiający odrzuca wniosek o dopuszczenie do udziału w postępowaniu o udzielnie zamówienia publicznego lub ofertę takiego wykonawcy lub uczestnika konkursu, nie zaprasza go do złożenia oferty wstępnej, oferty podlegającej negocjacjom, oferty dodatkowej, oferty lub oferty ostatecznej, nie zaprasza go do negocjacji lub dialogu, a także nie prowadzi z takim wykonawcą negocjacji lub dialogu, odrzuca wniosek o dopuszczenie do udziału w konkursie, nie zaprasza do złożenia pracy konkursowej lub nie przeprowadza oceny pracy konkursowej, odpowiednio do trybu stosowanego do udzielenia zamówienia publicznego oraz etapu prowadzonego postępowania o udzielenie zamówienia publicznego.
Osoba lub podmiot podlegające wykluczeniu na podstawie ust. 1, które w okresie tego wykluczenia ubiegają się o udzielenie zamówienia publicznego lub dopuszczenie do udziału w konkursie lub biorą udział w postępowaniu o udzielenie zamówienia publicznego lub w konkursie, podlegają karze pieniężnej.
Przez ubieganie się o udzielenie zamówienia publicznego lub dopuszczenie do udziału w konkursie rozumie się odpowiednio złożenie wniosku o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia publicznego lub konkursie, złożenie oferty, przystąpienie do negocjacji lub złożenie pracy konkursowej.
Wykonawca wraz z ofertą składa "oświadczenie o braku podstaw do wykluczenia na podstawie 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 (Dz. U. z 2022 r. poz. 835)" stanowiące załącznik nr 3 do SWZ.