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: 523241864

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-148610-35f32b15-4ae8-11ed-8832-4e4740e186ac

2.5.) Numer ogłoszenia: 2022/BZP 00391422/01

2.6.) Wersja ogłoszenia: 01

2.7.) Data ogłoszenia: 2022-10-13 13:45

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

2.9.) Numer planu postępowań w BZP: 2022/BZP 00019844/10/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.4.2022 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.4.2022

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

Część 1: Zakup macierzy dyskowej
Lp. Nazwa parametru Minimalna wartość parametru
1. Obudowa System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19"
2. Pojemność: System musi zostać dostarczony w konfiguracji zawierającej minimum:

12 dysków 4TB NL-SAS

oraz posiadać możliwość rozbudowy o kolejne dyski
System musi wspierać dyski:
• SAS: 900GB do 1800GB
• SATA/NL-SAS: od 4TB do 16TB
• SSD: 800GB do 7600GB
Budowa systemu musi umożliwiać rozbudowę do modeli wyższych bez potrzeby kopiowania/migrowania danych.
(zamawiający przez model wyższy rozumie inny model macierzy danego producenta z większą pamięcią cache oraz mocniejszymi procesorami).
Zamawiający dopuszcza rozwiązanie które nie pozwala na rozbudowę do wyższego modelu przy założeniu, że zostanie zaoferowany najwyższy model z rodziny z pamięcią Cache min 1TB na kontroler.
System musi mieć możliwość rozbudowy do 500 dysków w obrębie pary kontrolerów lub w obrębie klastra wielu kontrolerów

(scale-out) w zależności od sposobu realizacji rozbudowy dla oferowanego rozwiązania.
W przypadku klastrowania kontrolerów macierzy, system musi działać pod kontrolą jednego systemu operacyjnego od jednego producenta, nie dopuszczalne jest zestawienie systemu klastrowego poprzez wykorzystanie serwerów pośredniczących i oprogramowania dodatkowego.
Dla rozwiązań wykorzystujących klastrowanie (scale-out) musi być możliwość rozbudowy rozwiązania do co najmniej 12 kontrolerów w klastrze.
Rozwiązanie musi pozwalać na rozbudowę o dyski lub kontrolery wykonane w technologii NVMe do min 550 dysków w technologii NVME. Zamawiający dopuszcza zaoferowanie rozwiązania, które nie posiada takiej możliwości w przypadku gdy całość zasobów zostanie dostarczona na dyskach flash/SSD.
3. Kontroler Dwa kontrolery wyposażone w przynajmniej 256GB cache każdy.

Zamawiający dopuszcza alternatywnie rozwiązanie posiadające co najmniej 32GB cache oparte o RAM na kontroler jeżeli dodatkowo zostanie dostarczona z macierzą dodatkowa pamięć Flash minimum 1024GB pamięci na kontroler (wbudowana w kontroler lub formie dodatkowych dysków Flash skonfigurowanych w RAID 10)

Procesory macierzy powinny być wykonane w technologii wielordzeniowej z przynajmniej 12 rdzeniami na każdy kontroler dla procesorów AMD i Intel. Dla innych rodzajów procesorów min 64 rdzenie.
W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny lub poprzez zrzut na pamięć nieulotną
Macierz musi pozwalać na poszerzenie pamięci Cache za pomocą dysków SSD do 6TB.
4. Interfejsy Oferowana macierz musi posiadać minimum

8 portów 10GbE sfp+
2 porty 1Gb do zarządzania
4 porty 12Gb SAS,

5. RAID System RAID musi zapewniać taki poziom zabezpieczania danych, aby był możliwy do nich dostęp w sytuacji awarii minimum dwóch dysków w grupie RAID
6. Kopie Migawkowe Macierz musi być wyposażona w system kopii migawkowych, dostępny dla wszystkich rodzajów danych przechowywanych na macierzy. System kopii migawkowych nie może powodować spadku wydajności macierzy +/- 5%
7. Obsługiwane protokoły Macierz musi obsługiwać jednocześnie protokoły FC, iSCSi, CIFS i NFS, S3 (macierz obiektowa) - jeśli wymagane są licencje zamawiający wymaga dostarczenia ich wraz z macierzą.

8. Inne wymagania Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów Win 2003/2008, Linux, Vmware, Unix

Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie

Macierz musi posiadać funkcjonalność priorytetyzacji zadań.

Macierz musi posiadać funkcjonalność kompresji danych w trybie in-line oraz off-line na każdym rodzaju danych.

Macierz musi posiadać funkcjonalność eliminacji (deduplikacji) identycznych bloków danych którą można stosować na macierzy/danych produkcyjnej dla wszystkich rodzajów danych. Macierz powinna mieć możliwość czynności odwrotnej tzn. Cofnięcia procesu deduplikacji na zdeduplikowanym wolumenie. Jeżeli oferowane rozwiązanie nie posiada funkcjonalności deduplikacji danych, zamawiający wymaga dostarczenia 4-krotności przestrzeni wyspecyfikowanej.

Macierz musi posiadać funkcjonalność replikacji synchronicznej i asynchronicznej pomiędzy macierzami tego samego producenta. Funkcjonalność replikacji danych musi być natywnym narzędziem macierzy. Przed procesem replikacji macierz musi umożliwiać włączenie procesu deduplikacji danych w celu optymalizacji wykorzystania łącza dla replikowanych zasobów lub zamawiający wymaga dostarczenia zewnętrznego narzędzia do deduplikowania replikowanych danych lub dwukrotnego zwiększenia pojemności ze względu na rozważaną w przyszłości replikację całości zasobów.
Zamawiający dopuszcza zastosowanie zewnętrznego wirtualizatora (po 1 szt na replikowaną macierz) w celu spełnienia możliwości replikacji danych.

System musi pozwalać na rozbudowę o specjalny moduł do zabezpieczenia przez atakiem Ransomware w szczególności:
- musi informować administratora w przypadku nie standardowego zachowania systemu oraz danych
- wykonywać prewencyjną kopię migawkową „snapshot” w przypadku zagrożenia atakiem ransomware

Macierz musi posiadać możliwość automatycznego informowania przez macierz i przesyłania przez pocztę elektroniczną raportów o konfiguracji, utworzonych dyskach logicznych i woluminach oraz ich zajętości wraz z podziałem na rzeczywiste dane, kopie migawkowe oraz dane wewnętrzne macierzy.

Macierz musi posiadać funkcjonalność wykonania wirtualnych klonów, które nie wymagają kopiowania bloków danych.

Z macierzą zamawiający wymaga dostarczenia oprogramowania które pozwala na:
- monitoring wykorzystania przestrzeni na macierzy
- monitoring grup RAIDowych
- monitoring wykonywanych backupów/replikacji danych między macierzami
- monitoring wydajności macierzy
- analizę i diagnozę spadku wydajności
Zamawiający dopuszcza zastosowanie oprogramowania zewnętrznego, na pełną max pojemność macierzy.

Wszystkie funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy

Producent musi dostarczyć usługę w postaci portalu WWW lub dodatkowego oprogramowania umożliwiającą następujące funkcjonalności:
a) Narzędzie do tworzenia procedury aktualizacji oprogramowania macierzowego.
- procedura musi opierać się na aktualnych danych pochodzących z macierzy oraz najlepszych praktykach producenta.
- procedura musi uwzględniać systemy zależne np, macierze replikujące
- procedura musi umożliwiać generowanie planu cofnięcia aktualizacji.
b) Wyświetlanie statystyk dotyczących wydajności, utylizacji, oszczędności uzyskanych dzięki funkcjonalnościom macierzy.
c) Wyświetlanie konfiguracji macierzy oraz porównywanie jej z najlepszymi praktykami producenta w celu usunięcia błędów konfiguracji.

Portal lub oprogramowanie może pochodzić od innego producenta niż producent macierzy, z tym że zostanie dostarczona odpowiednia licencja do maksymalnej pojemności macierzy.

Zamawiający wymaga by wszystkie funkcjonalności działały wspólnie tj. włączenie jednej funkcjonalności nie eliminowało innej.

9. Gwarancja i serwis 3 lata serwisu producenta z 2 godzinnym czasem odpowiedzi na awarie krytyczne i dostawą elementów w na następny dzień roboczy

Zepsute dyski pozostają u zamawiającego

Dostarczony system musi posiadać również 3 lata subskrypcji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia.

10. Macierz musi posiadać funkcjonalność „Tieringu" zimnych danych na:
- inną macierz tego samego producenta (z wolnymi dyskami np. NL-SAS)
- inną macierz dowolnego producenta z protokołem S3
- Tiering musi być natywnym narzędziem macierzy i wykonywać się automatycznie.

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: 21 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

Część 2: Zakup urządzenia UTM
OBSŁUGA SIECI
1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
ZAPORA KORPORACYJNA (Firewall)
2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
INTRUSION PREVENTION SYSTEM (IPS)
12. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
13. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
14. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
15. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
16. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
17. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
18. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
19. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
20. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
KSZTAŁTOWANIE PASMA (Traffic Shapping)
21. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
22. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
23. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
24. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
OCHRONA ANTYWIRUSOWA
25. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).

26. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
27. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
28. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
OCHRONA ANTYSPAM
29. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
30. Ochrona antyspam ma działać w oparciu o:
a. białe/czarne listy,
b. DNS RBL,
c. Skaner heurystyczny.
31. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
32. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
WIRTUALNE SIECI PRYWATNE (VPN)
33. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
34. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
a. PPTP VPN,
b. IPSec VPN,
c. SSL VPN.
35. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
36. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
37. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
38. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
39. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
FILTR DOSTĘPU DO STRON WWW
40. Urządzenie ma posiadać wbudowany filtr URL.
41. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
42. Administrator ma mieć możliwość dodawania własnych kategorii URL.
43. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
a. blokowanie dostępu do adresu URL,
b. zezwolenie na dostęp do adresu URL,
c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
44. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
45. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
46. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
47. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
48. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
UWIERZYTELNIANIE
49. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
a. lokalną bazę użytkowników (wewnętrzny LDAP),
b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
c. usługę katalogową Microsoft Active Directory.
50. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
51. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
a. SSL,
b. Radius,
c. Kerberos.
52. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
53. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
54. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)
55. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
56. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
a. równoważenie względem adresu źródłowego,
b. równoważenie względem połączenia.
57. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.

58. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
59. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
60. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
61. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

62. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
63. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
64. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
65. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
ADMINISTRACJA URZĄDZENIEM
66. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
67. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
ciąg dalszy SWZ cz. II str. 9-11

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: 21 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

Część 3: Zakup i dostawa oprogramowania z licencją na Backup na 3 serwery fizyczne (w tym 6 virtrualnych), oraz 40 stacji roboczych

Wymagana funkcjonalność oprogramowania do Backup stacji roboczych:

1. Produkt i dokumentacja dostępna w polskiej (i angielskiej) wersji językowej
2. Produkt z licencją dożywotnią
3. Aktualizacja oprogramowania na min 1 rok
4. Wsparcie dla systemów operacyjnych Windows typu stacja robocza:
Systemy operacyjne Windows: Windows 8/8.1, Windows XP, Windows Vista, Windows 7, Windows 10, Windows 11

5. Wsparcie i pełna funkcjonalność oprogramowania dla wielojęzykowych systemów operacyjnych
6. Tworzenie kopii zapasowych dysków/partycji
7. Tworzenie kopii zapasowych plików i folderów
8. Replikacja kopii zapasowych do wielu lokalizacji docelowych
9. Tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
10. Możliwość przywrócenia kopii zapasowej dysku/partycji na innym komputerze o innej konfiguracji sprzętowej
11. Obsługa dysków twardych z sektorami o rozmiarze 4KB oraz dysków SSD
12. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej
13. Zdalna instalacja i aktualizacja agentów na komputerach klienckich
14. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych oraz serwerach SFTP
15. Obsługa napędów taśmowych.
16. Deduplikacja kopii zapasowych.
17. Możliwość generowania planu przywracania kopii zapasowych
18. Możliwość eksportu i importu planów tworzenia kopii zapasowych na różnych maszynach
19. Szablony schematów rotacji kopii zapasowych
20. Polecenia poprzedzające/następujące
21. Automatyczne usuwanie nieaktualnych kopii zapasowych (retencja)
22. Sprawdzanie poprawności i konsolidacja kopii zapasowych (pełnych, przyrostowych i różnicowych)
23. Wykonywanie zadań i tworzenie kopii zapasowych możliwe z poziomu wiersza polecenia.
24. Możliwość utworzenia ukrytej partycji widzianej tylko przez oprogramowanie do backupu na potrzeby zapisu kopii zapasowych, która będzie chroniona za pomocą hasła
25. Współpraca z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
26. Pełne, przyrostowe i różnicowe kopie zapasowe
27. Wysyłanie powiadomień pocztą e-mail
28. Szyfrowane kopii zapasowych algorytmem AES
29. Możliwość wykonywania czynności przenoszenia kopii zapasowych, replikacji, weryfikacji i czyszczenia na innym systemie.
30. Funkcjonalność ciągłej ochrony danych
31. Analiza podatności urządzenia (poszukiwanie luk w oprogramowaniu objętym ochroną), środowisko Windows
32. Funkcja aktywnej ochrony przed oprogramowaniem ransomware, chroniąca pliki lokalne i pliki kopii zapasowych przed zaszyfrowaniem.
33. Predefiniowany schemat tworzenia kopii zapasowych: G-F-S
34. Priorytetowe przywracanie systemu operacyjnego - Jeśli system uległ awarii, można go uruchomić w ciągu kilku sekund, a proces przywracania będzie wykonywany w tle.
35. Uruchamianie usług z minimalnymi prawami użytkownika
36. Zaawansowane raportowanie - możliwość tworzenia raportów w oparciu o predefiniowane schematy
37. Pomoc techniczna dostępna w języku polskim
38. Administrowanie kontami użytkowników Acronis i jednostkami organizacyjnymi
39. Tworzenie kryptograficznego odcisku pliku (sumy kontrolnej) wykorzystującego technologię blockchain
40. Wykonywanie kopii zapasowych uruchamiane po wystąpieniu określonych zdarzeń i warunków
41. Migawki wielowoluminowe
42. Kopia zapasowa „sektor po sektorze"
43. Obsługa dysków dynamicznych

Wymagana funkcjonalność oprogramowania do Backup Serwerów:

1. Produkt i dokumentacja dostępna w polskiej (i angielskiej) wersji językowej
2. Wsparcie dla środowisk wirtualizacji: Hyper-V, VMware vSphere, Citrix XenServer, Red Hat Virtualization, Linux KVM I Oracle VM Server
3. Obsługa aplikacji MS SQL, MS Exchange, AD, SharePoint, BD Oracle,
4. Wsparcie i pełna funkcjonalność oprogramowania dla wielojęzykowych systemów operacyjnych
5. Obsługa środowiska chmurowego
6. Tworzenie kopii zapasowych dysków/partycji
7. Tworzenie kopii zapasowych plików i folderów
8. Replikacja kopii zapasowych do wielu lokalizacji docelowych
9. Tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
10. Możliwość przywrócenia kopii zapasowej dysku/partycji na innym komputerze o innej konfiguracji sprzętowej
11. Obsługa dysków twardych z sektorami o rozmiarze 4KB oraz dysków SSD
12. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej
13. Zdalna instalacja i aktualizacja agentów na komputerach klienckich
14. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych oraz serwerach SFTP
15. Obsługa napędów taśmowych.
16. Deduplikacja kopii zapasowych.
17. Możliwość generowania planu przywracania kopii zapasowych
18. Możliwość eksportu i importu planów tworzenia kopii zapasowych na różnych maszynach

19. Szablony schematów rotacji kopii zapasowych
20. Polecenia poprzedzające/następujące
21. Automatyczne usuwanie nieaktualnych kopii zapasowych (retencja)
22. Sprawdzanie poprawności i konsolidacja kopii zapasowych (pełnych, przyrostowych i różnicowych)
23. Wykonywanie zadań i tworzenie kopii zapasowych możliwe z poziomu wiersza polecenia.
24. Możliwość utworzenia ukrytej partycji widzianej tylko przez oprogramowanie do backupu na potrzeby zapisu kopii zapasowych, która będzie chroniona za pomocą hasła
25. Współpraca z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
26. Pełne, przyrostowe i różnicowe kopie zapasowe
27. Wysyłanie powiadomień pocztą e-mail
28. Szyfrowane kopii zapasowych algorytmem AES
29. Możliwość wykonywania czynności przenoszenia kopii zapasowych, replikacji, weryfikacji i czyszczenia na innym systemie.
30. Funkcjonalność ciągłej ochrony danych
31. Analiza podatności urządzenia (poszukiwanie luk w oprogramowaniu objętym ochroną), środowisko Windows

Funkcjonalność unikalna:

32. Funkcja aktywnej ochrony przed oprogramowaniem ransomware, chroniąca pliki lokalne i pliki kopii zapasowych przed zaszyfrowaniem.
33. Predefiniowany schemat tworzenia kopii zapasowych: G-F-S
34. Priorytetowe przywracanie systemu operacyjnego - Jeśli system uległ awarii, można go uruchomić w ciągu kilku sekund, a proces przywracania będzie wykonywany w tle.
35. Uruchamianie usług z minimalnymi prawami użytkownika
36. Zaawansowane raportowanie - możliwość tworzenia raportów w oparciu o predefiniowane schematy
37. Pomoc techniczna dostępna w języku polskim
38. Administrowanie kontami użytkowników Acronis i jednostkami organizacyjnymi
39. Tworzenie kryptograficznego odcisku pliku (sumy kontrolnej) wykorzystującego technologię blockchain

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: 21 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

Art. 109 ust. 1 pkt 9

Art. 109 ust. 1 pkt 10

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)
2.3. 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.
2.4. Przepisy dotyczące Wykonawcy stosuje się odpowiednio do wykonawców wspólnie ubiegających się o udzielenie zamówienia.
2.5. 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: 2022-10-24 12:00

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: 2022-10-24 13:00

8.4.) Termin związania ofertą: do 2022-11-22

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.