Ogłoszenie o zamówieniu
Usługi
Wdrożenie usług z zakresu cyberbezpieczeństwa

SEKCJA I - ZAMAWIAJĄCY

1.1.) Rola zamawiającego

Postępowanie prowadzone jest samodzielnie przez zamawiającego

1.2.) Nazwa zamawiającego: Gmina Rudniki

1.4) Krajowy Numer Identyfikacyjny: REGON 151398586

1.5) Adres zamawiającego

1.5.1.) Ulica: Wojska Polskiego 12A

1.5.2.) Miejscowość: Rudniki

1.5.3.) Kod pocztowy: 46-325

1.5.4.) Województwo: opolskie

1.5.5.) Kraj: Polska

1.5.6.) Lokalizacja NUTS 3: PL524 - Opolski

1.5.7.) Numer telefonu: 34 3595072

1.5.9.) Adres poczty elektronicznej: przetargi@rudniki.pl

1.5.10.) Adres strony internetowej zamawiającego: www.rudniki.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:

Wdrożenie usług z zakresu cyberbezpieczeństwa

2.4.) Identyfikator postępowania: ocds-148610-95ee2e15-9208-4ed9-a33c-cb84a7d7446f

2.5.) Numer ogłoszenia: 2024/BZP 00538024

2.6.) Wersja ogłoszenia: 01

2.7.) Data ogłoszenia: 2024-10-09

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

2.9.) Numer planu postępowań w BZP: 2023/BZP 00577880/13/P

2.10.) Identyfikator pozycji planu postępowań:

1.3.2 Wdrożenie usług z zakresu cyberbezpieczeństwa

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

"Cyberbezpieczny samorząd”, który jest realizowany w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój

Cyfrowy 2021 – 2027 (FERC) Działanie 2.2 - Wzmocnienie krajowego systemu cyberbezpieczeństwa.

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
https://platformazakupowa.pl/pn/rudniki

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: Postępowanie prowadzone jest w języku polskim, w formie elektronicznej za pośrednictwem Platformy Zakupowej pod adresem: https://platformazakupowa.pl/pn/rudniki.
Zamawiający dopuszcza, opcjonalnie komunikację między Zamawiającym a Wykonawcą przy użyciu: ePUAP:/GminaRudniki/SkrytkaESP oraz poczty elektronicznej: przetargi@rudniki.pl (za wyjątkiem oferty (zał. Nr 1 do SWZ) i oświadczeń wstępnych z art. 125ustawy Pzp (zał. Nr 4 do SWZ), które obligatoryjnie składane są za pośrednictwem Platformy zakupowej.
Zgodnie z art. 61 ust 2 ustawy Pzp komunikacja ustna dopuszczalna jest jedynie w toku negocjacji lub dialogu oraz w odniesieniu do informacji, które nie są istotne.

3.6.) Wymagania techniczne i organizacyjne dotyczące korespondencji elektronicznej: Preferuje się aby komunikacja miedzy Zamawiającym a Wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje, przekazywane były w formie elektronicznej za pośrednictwem platformazakupowa.pl i formularza „Wyślij wiadomość do zamawiającego”.
Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem platformazakupowa.pl poprzez kliknięcie przycisku „Wyślij wiadomość do zamawiającego”, po którym pojawi się komunikat, że wiadomość została wysłana do zamawiającego. Zamawiający dopuszcza, opcjonalnie, komunikację za pośrednictwem poczty elektronicznej: przetargi@rudniki.pl.
Zamawiający będzie przekazywał wykonawcom informacje za pośrednictwem platformazakupowa.pl. Informacje dotyczące odpowiedzi na pytania, zmiany specyfikacji, zmiany terminu składania i otwarcia ofert – kierowanie do ogółu zainteresowanych Zamawiający będzie zamieszczał na Platformie w sekcji „ Komunikaty”. Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny Wykonawca, będzie przekazywana za pośrednictwem platformazakupowa.pl do konkretnego wykonawcy.
Do komunikowania się z Wykonawcami uprawnieni są Daniel Pilak i Karolina Majka.
W przypadku pytań technicznych dotyczących funkcjonowania i obsługi technicznej Platformy Zakupowej wskazuje kontakt z Centrum Wsparcia Klienta, które udziela wszelkich informacji związanych z procesem składania ofert, rejestracji oraz innych aspektów technicznych Platformy. Centrum wsparcia Klienta dostępne jest od poniedziałku do piątku w godz.: od 7:00 do 17:00 pod numerem telefonu (22)-101-02-02 lub e-mail cwk@platformazakupowa.pl.
Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na platformazakupowa.pl przesłanych przez Zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.
Zgodnie z art. 67 ustawy Pzp Zamawiający podaje wymagania techniczne związane z korzystaniem z Platformy:
1) stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
2) komputer klasy PC lub MAC o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10 4, Linux, lub ich nowsze wersje,
3) zainstalowana dowolna przeglądarka internetowa, w przypadku Internet Explorer minimalnie wersja 10 0.,
4) włączona obsługa JavaScript,
5) zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf, Platformazakupowa.pl działa według standardu przyjętego w komunikacji sieciowej - kodowanie UTF8,
Oznaczenie czasu odbioru danych przez platformę zakupową stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.
Pozostałe wymagania zostały zawarte w Rozdziale XIII SWZ.

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 i 2 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 (ogólne rozporządzenie o danych) (Dz. U. UE L119 z dnia 4 maja 2016 r., str. 1; zwanym dalej „RODO”) informujemy, że:
1) administratorem Pani/Pana danych osobowych jest Wójt Gminy Rudniki

3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z przedmiotowym postępowaniem o udzielenie zamówienia publicznego, prowadzonym w trybie podstawowym bez negocjacji
4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 74 ustawy PZP
5) Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 PZP przez okres 4 lat od dnia 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.
7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO.
8) posiada Pani/Pan:
a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących (w przypadku, gdy skorzystanie z tego prawa wymagałoby po stronie administratora niewspółmiernie dużego wysiłku może zostać Pani/Pan zobowiązana do wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego lub konkursu albo sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia);
b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych (skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą PZP oraz nie może naruszać integralności protokołu oraz jego załączników);
c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem okresu trwania postępowania o udzielenie zamówienia publicznego lub konkursu oraz przypadków, o których mowa w art. 18 ust. 2 RODO (prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego);
d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
9) nie przysługuje Pani/Panu:
a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
c) na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO;
10) przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Pana danych osobowych przez administratora. Organem właściwym dla przedmiotowej skargi jest Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.
Pełna klauzula RODO znajduje się w Rozdziale II SWZ.

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: PRG.271.16.2024

4.1.3.) Rodzaj zamówienia: Usługi

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: 4

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 I: Świadczenie usług utrzymania środowiska SIEM/SOC wraz z dostawą i wdrożeniem serwera:
1) Świadczenie usług utrzymania systemu Zarządzania Informacjami i Zdarzeniami Bezpieczeństwa (SIEM) oraz Centrum Operacji Bezpieczeństwa (SOC)
a) Skonfigurowanie w ramach platformy witalizacyjnej funkcjonalności kopii zapasowych i odzyskiwania plików i danych oprogramowania dla środowiska SIEM/SOC
b) Opracowanie i wdrożenie planu zarządzania podatnościami. Wykonawca opracuje i przedstawi plan działania na wypadek krytycznych incydentów bezpieczeństwa, który będzie obejmował:
i. Procedury natychmiastowej reakcji na incydenty,

ii. Procedury powiadamiania odpowiednich służb i zespołów reagowania,
iii. Plany przywracania działania systemów po incydentach,
iv. Procedury analizy incydentów po ich wystąpieniu oraz wdrażania działań zapobiegawczych.
c) Monitorowanie, analiza oraz odpowiedź na incydenty bezpieczeństwa w postaci przekazania pełnej informacji do zespołu IT Zleceniodawcy
d) Sporządzanie okresowych raportów:
i. Comiesięczne raporty szczegółowe z działania systemu SOC/SIEM (18 raportów w ciągu 18 miesięcy)
ii. Kwartalne raporty podsumowujące (1-2 strony) z zaleceniami
e) Wdrożenie zaleceń z raportów kwartalnych, wykonane przez 2-osobowy zespół Wykonawcy w ścisłej współpracy z zespołem IT Zamawiającego
2) Dostawa i wdrożenie serwera wraz z oprogramowaniem dla środowiska SIEM/SOC – obejmujące dostawę, instalację oraz konfigurację sprzętu komputerowego, zgodnie z określoną specyfikacją techniczną.
Szczegółowy opis znajduje się się w Opisie przedmiotu zamówienia - załącznik nr 6 do SWZ.

4.2.6.) Główny kod CPV: 72611000-6 - Usługi w zakresie wsparcia technicznego

4.2.7.) Dodatkowy kod CPV:

72250000-2 - Usługi w zakresie konserwacji i wsparcia systemów

30211000-1 - Komputery wysokowydajne

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: 18 miesiące

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: Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującymi kryteriami oceny ofert (dla każdej z części zamówienia):
Lp. Nazwa kryterium Waga
1 Cena (C) 60 %
2 Ilość lat posiadania kwalifikacji w branży „IT Security” jednej osoby wyznaczonej do realizacji zamówienia(K) 40 %
Zasady oceny ofert w poszczególnych kryteriach:
1) Kryterium Cena (C) – waga 60 %
C=(Cena najniższa brutto*/Cena ocenianej oferty brutto)x100x60 %
*spośród wszystkich złożonych ofert niepodlegających odrzuceniu
a) Podstawą przyznania punktów o kryterium Cena będzie cena ofertowa brutto podana przez Wykonawcę w Formularzu Ofertowym.
b) Cena ofertowa brutto musi uwzględniać wszelkie koszty jakie Wykonawca poniesie w związku z realizacją przedmiotu zamówienia.
c) W kryterium Cena można uzyskać maksymalnie 60 punktów od jednego członka komisji przetargowej. Przyznane punkty zostaną zaokrąglone do dwóch miejsc po przecinku.
2) Kryterium Ilość lat posiadania kwalifikacji w branży „IT Security” jednej osoby wyznaczonej do realizacji zamówienia(K) – waga 40 %
Zamawiający ocenia ilość lat posiadania kwalifikacji w branży „IT Security” liczona w latach od daty wystawienia branżowego certyfikatu (CEH, CCNP Security, CCIE Security, CCNA CyberOps, PCNSE, FCX in Cybersecurity lub równoważnego pod względem zakresu certyfikacji) osoby oddelegowanej do realizacji zamówienia. Za rok przyjmuje się 365 dni. Minimalny okres posiadania kwalifikacji Zamawiający ustala na 3 lata.
Ilość lat od 3 lat do 4 lat 10 punktów;
Ilość lat powyżej 4 lat do 5 lat 20 punktów;
Ilość lat powyżej 5 lat do 6 lat 30 punktów;
Ilość lat powyżej 6 lat 40 punktów;
Zaoferowanie przez Wykonawcę osoby oddelegowanej do realizacji zamówienia z brakiem kwalifikacji potwierdzonych certyfikatem lub poniżej 3 lat spowoduje odrzucenie oferty, jako treść niezgodna z warunkami zamówienia – art. 226 ust 1 pkt 5 ustawy Pzp. Brak określenia przez Wykonawcę ilości lat posiadania kwalifikacji osoby wyznaczonej do realizacji zamówienia spowoduje odrzucenie oferty, jako treść niezgodna z warunkami zamówienia – art. 226 ust 1 pkt 5 ustawy Pzp.
Łączna ocena ofert:
W = C + K
W – wskaźnik oceny oferty
C – ilość punktów przyznanych ofercie w kryterium Cena;
K – ilość punktów przyznanych ofercie w kryterium Ilość lat posiadania kwalifikacji w branży „IT Security” jednej osoby wyznaczonej do realizacji zamówienia.
Punktacja przyznawana ofertom w poszczególnych kryteriach oceny ofert będzie liczona z dokładnością do dwóch miejsc po przecinku, zgodnie z zasadami arytmetyki.
Maksymalna ilość punktów, jaką może otrzymać oferta wynosi 100 punktów od 1 członka komisji przetargowej. Po dokonaniu oceny

ofert punkty przyznane przez każdego z członków komisji przetargowej będą zsumowane dla każdego z kryteriów oddzielnie. Jeżeli nie można wybrać oferty najkorzystniejszej z uwagi na to, że dwie lub więcej ofert przedstawi taki sam wskaźnik oceny ofert, Zamawiający spośród tych ofert wybierze ofertę z niższą ceną.

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: organizacja, kwalifikacje zawodowe i doświadczenie osób wyznaczonych do realizacji zamówienia

4.3.5.) Nazwa kryterium: Ilość lat posiadania kwalifikacji w branży „IT Security" jednej osoby wyznaczonej do realizacji zamówienia(K)

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 II: Audyt bezpieczeństwa infrastruktury IT zgodny z wymogami Krajowych Ram Interoperacyjności (KRI) oraz wdrożenie zaleceń poaudytowych:
Przedmiotem zamówienia jest przeprowadzenie audytu bezpieczeństwa infrastruktury IT zgodnego z wymogami Krajowych Ram Interoperacyjności (KRI) oraz wdrożenie zaleceń poaudytowych w organizacji Zamawiającego. Celem audytu jest zidentyfikowanie potencjalnych luk i słabości w systemach, aplikacjach oraz konfiguracjach urządzeń sieciowych, a następnie wdrożenie odpowiednich środków zaradczych, aby zapewnić zgodność z aktualnymi standardami bezpieczeństwa systemów teleinformatycznych.
1) Audyt bezpieczeństwa infrastruktury IT:
a) Przegląd i analiza aktualnej infrastruktury IT
i. Dokumentacja i schematy topologii sieci
ii. Inwentaryzacja urządzeń i systemów
b) Przegląd architektury sieci pod kątem bezpieczeństwa teleinformatycznego
i. Analiza segmentacji sieci
ii. Ocena mechanizmów kontroli dostępu
c) Ocena polityk bezpieczeństwa i procedur, w szczególności przeprowadzenie audytu polityki kopii zapasowych i backupów, audyt procedur na wypadek awarii
i. Przegląd polityk zarządzania hasłami
ii. Ocena procedur zarządzania incydentami
d) Testy penetracyjne wewnętrzne i analiza podatności
i. Analiza zabezpieczeń urządzeń sieciowych
ii. Analiza podatności systemów operacyjnych
iii. Testy aplikacji webowych i usług sieciowych
e) Testy penetracyjne zewnętrzne i analiza podatności
i. Testy zabezpieczeń firewalli i routerów
ii. Symulacja ataków z zewnątrz
f) Przegląd konfiguracji urządzeń sieciowych i usług
i. Ocena zabezpieczeń protokołów sieciowych
ii. Sprawdzenie konfiguracji urządzeń pod kątem zgodności z najlepszymi praktykami
g) Ocena zgodności z KRI
2) Przygotowanie raportu z audytu:
a) Szczegółowy raport zawierający wyniki audytu
b) Wizualizacja luk i podatności na schematach sieci
c) Identyfikacja luk i podatności w systemach wraz z wyjaśnieniem ich znaczenia i oceną ryzyka (prawdopodobieństwo/zagrożenie)
d) Określenie priorytetów dla działań naprawczych
e) Wnioski i rekomendacje w celu dokładnego rozpoznania i redukcji zidentyfikowanych ryzyka, zagrożeń i podatności oraz wskazanie adekwatnych działań (zaleceń) mających na celu jak najszybsze ich wyeliminowanie
3) Wdrożenie zaleceń, wykonane przez 3-osobowy zespół Wykonawcy w ścisłej współpracy z zespołem IT Zamawiającego:
a) Analiza możliwości technicznych implementacji zaleceń, pod względem urządzeń, konfiguracji, licencji, ciągłości działania sieci i ciągłości dostępu do usług.

b) Dostosowanie infrastruktury do wdrożenia zaleceń
i. Modyfikacja konfiguracji sieci
ii. Aktualizacja oprogramowania i firmware'u
c) Przygotowanie scenariuszy wdrożenia zaleceń, wraz z procedurami roll-back
d) Wykonanie kopii zapasowych wraz z testami odtworzeniowymi
e) Kontrolowane wdrożenie zaleceń w oknach serwisowych (22:00 – 6:00)
f) Monitorowanie i weryfikacja wdrożonych zaleceń
4) Przygotowanie raportu z wdrożenia zaleceń.
Szczegółowy opis znajduje się się w Opisie przedmiotu zamówienia - załącznik nr 6 do SWZ.

4.2.6.) Główny kod CPV: 72800000-8 - Usługi audytu komputerowego i testowania komputerów

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: 3 miesiące

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: Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującymi kryteriami oceny ofert (dla każdej z części zamówienia):
Lp. Nazwa kryterium Waga
1 Cena (C) 60 %
2 Ilość lat posiadania kwalifikacji w branży „IT Security" jednej osoby wyznaczonej do realizacji zamówienia(K) 40 %
Zasady oceny ofert w poszczególnych kryteriach:
1) Kryterium Cena (C) – waga 60 %
C=(Cena najniższa brutto*/Cena ocenianej oferty brutto)x100x60 %
*spośród wszystkich złożonych ofert niepodlegających odrzuceniu
a) Podstawą przyznania punktów o kryterium Cena będzie cena ofertowa brutto podana przez Wykonawcę w Formularzu Ofertowym.
b) Cena ofertowa brutto musi uwzględniać wszelkie koszty jakie Wykonawca poniesie w związku z realizacją przedmiotu zamówienia.
c) W kryterium Cena można uzyskać maksymalnie 60 punktów od jednego członka komisji przetargowej. Przyznane punkty zostaną zaokrąglone do dwóch miejsc po przecinku.
2) Kryterium Ilość lat posiadania kwalifikacji w branży „IT Security" jednej osoby wyznaczonej do realizacji zamówienia(K) – waga 40 %
Zamawiający ocenia ilość lat posiadania kwalifikacji w branży „IT Security" liczona w latach od daty wystawienia branżowego certyfikatu (CEH, CCNP Security, CCIE Security, CCNA CyberOps, PCNSE, FCX in Cybersecurity lub równoważnego pod względem zakresu certyfikacji) osoby oddelegowanej do realizacji zamówienia. Za rok przyjmuje się 365 dni. Minimalny okres posiadania kwalifikacji Zamawiający ustala na 3 lata.
Ilość lat od 3 lat do 4 lat 10 punktów;
Ilość lat powyżej 4 lat do 5 lat 20 punktów;
Ilość lat powyżej 5 lat do 6 lat 30 punktów;
Ilość lat powyżej 6 lat 40 punktów;
Zaoferowanie przez Wykonawcę osoby oddelegowanej do realizacji zamówienia z brakiem kwalifikacji potwierdzonych certyfikatem lub poniżej 3 lat spowoduje odrzucenie oferty, jako treść niezgodna z warunkami zamówienia – art. 226 ust 1 pkt 5 ustawy Pzp. Brak określenia przez Wykonawcę ilości lat posiadania kwalifikacji osoby wyznaczonej do realizacji zamówienia spowoduje odrzucenie oferty, jako treść niezgodna z warunkami zamówienia – art. 226 ust 1 pkt 5 ustawy Pzp.
Łączna ocena ofert:
W = C + K
W – wskaźnik oceny oferty
C – ilość punktów przyznanych ofercie w kryterium Cena;
K – ilość punktów przyznanych ofercie w kryterium Ilość lat posiadania kwalifikacji w branży „IT Security" jednej osoby wyznaczonej do realizacji zamówienia.
Punktacja przyznawana ofertom w poszczególnych kryteriach oceny ofert będzie liczona z dokładnością do dwóch miejsc po przecinku, zgodnie z zasadami arytmetyki.
Maksymalna ilość punktów, jaką może otrzymać oferta wynosi 100 punktów od 1 członka komisji przetargowej. Po dokonaniu oceny ofert punkty przyznane przez każdego z członków komisji przetargowej będą zsumowane dla każdego z kryteriów oddzielnie.
Jeżeli nie można wybrać oferty najkorzystniejszej z uwagi na to, że dwie lub więcej ofert przedstawi taki sam wskaźnik oceny ofert, Zamawiający spośród tych ofert wybierze ofertę z niższą ceną.

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: organizacja, kwalifikacje zawodowe i doświadczenie osób wyznaczonych do realizacji zamówienia

4.3.5.) Nazwa kryterium: Ilość lat posiadania kwalifikacji w branży „IT Security" jednej osoby wyznaczonej do realizacji zamówienia(K)

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 III: Usługa szkoleniowa z zakresu Cyberbezpieczeństwa:
Przedmiotem zamówienia jest przeprowadzenie 12 szkoleń z tematyki Cyberbezpieczeństwa dla pracowników Urzędu Gminy na przestrzeni 18 miesięcy:
1) ABC Cyberbezpieczeństwa, czas trwania: 2h zegarowe, 4 szkolenia
2) Liderzy Cyberbezpieczeństwa: Szkolenie dla Zarządu, czas trwania: 2h zegarowe, 4 szkolenia
3) Bezpieczeństwo Infrastruktury IT, czas trwania: 2h zegarowe, 4 szkolenia
Szczegółowy opis znajduje się się w Opisie przedmiotu zamówienia - załącznik nr 6 do SWZ.

4.2.6.) Główny kod CPV: 80500000-9 - Usługi szkoleniowe

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: 18 miesiące

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: Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującymi kryteriami oceny ofert (dla każdej z części zamówienia):
Lp. Nazwa kryterium Waga
1 Cena (C) 60 %
2 Ilość lat posiadania kwalifikacji w branży „IT Security" jednej osoby wyznaczonej do realizacji zamówienia(K) 40 %
Zasady oceny ofert w poszczególnych kryteriach:
1) Kryterium Cena (C) – waga 60 %
C=(Cena najniższa brutto*/Cena ocenianej oferty brutto)x100x60 %
*spośród wszystkich złożonych ofert niepodlegających odrzuceniu
a) Podstawą przyznania punktów o kryterium Cena będzie cena ofertowa brutto podana przez Wykonawcę w Formularzu Ofertowym.
b) Cena ofertowa brutto musi uwzględniać wszelkie koszty jakie Wykonawca poniesie w związku z realizacją przedmiotu zamówienia.
c) W kryterium Cena można uzyskać maksymalnie 60 punktów od jednego członka komisji przetargowej. Przyznane punkty zostaną zaokrąglone do dwóch miejsc po przecinku.
2) Kryterium Ilość lat posiadania kwalifikacji w branży „IT Security" jednej osoby wyznaczonej do realizacji zamówienia(K) – waga 40 %
Zamawiający ocenia ilość lat posiadania kwalifikacji w branży „IT Security" liczona w latach od daty wystawienia branżowego certyfikatu (CEH, CCNP Security, CCIE Security, CCNA CyberOps, PCNSE, FCX in Cybersecurity lub równoważnego pod względem zakresu certyfikacji) osoby oddelegowanej do realizacji zamówienia. Za rok przyjmuje się 365 dni. Minimalny okres posiadania kwalifikacji Zamawiający ustala na 3 lata.
Ilość lat od 3 lat do 4 lat 10 punktów;
Ilość lat powyżej 4 lat do 5 lat 20 punktów;
Ilość lat powyżej 5 lat do 6 lat 30 punktów;
Ilość lat powyżej 6 lat 40 punktów;
Zaoferowanie przez Wykonawcę osoby oddelegowanej do realizacji zamówienia z brakiem kwalifikacji potwierdzonych certyfikatem lub poniżej 3 lat spowoduje odrzucenie oferty, jako treść niezgodna z warunkami zamówienia – art. 226 ust 1 pkt 5 ustawy Pzp. Brak określenia przez Wykonawcę ilości lat posiadania kwalifikacji osoby wyznaczonej do realizacji zamówienia spowoduje odrzucenie oferty, jako treść niezgodna z warunkami zamówienia – art. 226 ust 1 pkt 5 ustawy Pzp.
Łączna ocena ofert:
W = C + K
W – wskaźnik oceny oferty
C – ilość punktów przyznanych ofercie w kryterium Cena;

K – ilość punktów przyznanych ofercie w kryterium Ilość lat posiadania kwalifikacji w branży „IT Security” jednej osoby wyznaczonej do realizacji zamówienia.
Punktacja przyznawana ofertom w poszczególnych kryteriach oceny ofert będzie liczona z dokładnością do dwóch miejsc po przecinku, zgodnie z zasadami arytmetyki.
Maksymalna ilość punktów, jaką może otrzymać oferta wynosi 100 punktów od 1 członka komisji przetargowej. Po dokonaniu oceny ofert punkty przyznane przez każdego z członków komisji przetargowej będą zsumowane dla każdego z kryteriów oddzielnie.
Jeżeli nie można wybrać oferty najkorzystniejszej z uwagi na to, że dwie lub więcej ofert przedstawi taki sam wskaźnik oceny ofert, Zamawiający spośród tych ofert wybierze ofertę z niższą ceną.

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: organizacja, kwalifikacje zawodowe i doświadczenie osób wyznaczonych do realizacji zamówienia

4.3.5.) Nazwa kryterium: Ilość lat posiadania kwalifikacji w branży „IT Security” jednej osoby wyznaczonej do realizacji zamówienia(K)

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 4

4.2.2.) Krótki opis przedmiotu zamówienia

Część IV: Zabezpieczenie infrastruktury IT – Device Hardening:
Przedmiotem zamówienia jest usługa zabezpieczenia infrastruktury IT poprzez zastosowanie procesu device hardening (uszczelnienia urządzeń) w celu zwiększenia odporności na potencjalne zagrożenia. Usługa obejmuje szereg działań mających na celu zmniejszenie powierzchni ataku oraz wdrożenie mechanizmów ochrony w urządzeniach takich jak: Serwery fizyczne i wirtualne (do 4 sztuk),Routery i firewalle (do 4 sztuk), Przełączniki sieciowe L2 i L3 (do 12 sztuk), Inne urządzenia sieciowe (drukarki, kamery IP, itp.) (do 5 sztuk).
Usługa device hardening obejmuje następujące działania:
1) Analiza i inwentaryzacja urządzeń:
a) Identyfikacja wszystkich urządzeń wchodzących w skład infrastruktury IT
b) Określenie typu, modelu, systemu operacyjnego i roli każdego urządzenia
c) Analiza konfiguracji urządzeń pod kątem potencjalnych luk w zabezpieczeniach
2) Opracowanie planu zabezpieczeń:
a) Opracowanie indywidualnego planu device hardening dla każdego typu urządzenia
b) Uwzględnienie specyfiki i wymagań poszczególnych urządzeń oraz całej infrastruktury
c) Konsultacje z Zamawiającym w celu dostosowania planu do jego potrzeb
3) Wdrożenie zabezpieczeń:
a) Wyłączenie zbędnych usług i protokołów
b) Aktualizacja oprogramowania i firmware'u do najnowszych wersji
c) Utworzenie i egzekwowanie polityki silnych haseł
d) Wdrożenie mechanizmów uwierzytelniania dwuskładnikowego (2FA)
e) Konfiguracja logowania i monitorowania zdarzeń
f) Wdrożenie mechanizmów ochrony przed atakami DDoS
g) Inne działania mające na celu zwiększenie bezpieczeństwa urządzeń
4) Testowanie i weryfikacja:
a) Przeprowadzenie testów penetracyjnych w celu weryfikacji skuteczności wdrożonych zabezpieczeń
b) Analiza wyników testów i ewentualne wprowadzenie dodatkowych zabezpieczeń
c) Sporządzenie raportu z testów i rekomendacji.
Szczegółowy opis znajduje się się w Opisie przedmiotu zamówienia - załącznik nr 6 do SWZ.

4.2.6.) Główny kod CPV: 72250000-2 - Usługi w zakresie konserwacji i wsparcia systemów

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: 2 miesiące

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: Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującymi kryteriami oceny ofert (dla każdej z części zamówienia):
Lp. Nazwa kryterium Waga
1 Cena (C) 60 %
2 Ilość lat posiadania kwalifikacji w branży „IT Security" jednej osoby wyznaczonej do realizacji zamówienia(K) 40 %
Zasady oceny ofert w poszczególnych kryteriach:
1) Kryterium Cena (C) – waga 60 %
C=(Cena najniższa brutto*/Cena ocenianej oferty brutto)x100x60 %
*spośród wszystkich złożonych ofert niepodlegających odrzuceniu
a) Podstawą przyznania punktów o kryterium Cena będzie cena ofertowa brutto podana przez Wykonawcę w Formularzu Ofertowym.
b) Cena ofertowa brutto musi uwzględniać wszelkie koszty jakie Wykonawca poniesie w związku z realizacją przedmiotu zamówienia.
c) W kryterium Cena można uzyskać maksymalnie 60 punktów od jednego członka komisji przetargowej. Przyznane punkty zostaną zaokrąglone do dwóch miejsc po przecinku.
2) Kryterium Ilość lat posiadania kwalifikacji w branży „IT Security" jednej osoby wyznaczonej do realizacji zamówienia(K) – waga 40 %
Zamawiający ocenia ilość lat posiadania kwalifikacji w branży „IT Security" liczona w latach od daty wystawienia branżowego certyfikatu (CEH, CCNP Security, CCIE Security, CCNA CyberOps, PCNSE, FCX in Cybersecurity lub równoważnego pod względem zakresu certyfikacji) osoby oddelegowanej do realizacji zamówienia. Za rok przyjmuje się 365 dni. Minimalny okres posiadania kwalifikacji Zamawiający ustala na 3 lata.
Ilość lat od 3 lat do 4 lat 10 punktów;
Ilość lat powyżej 4 lat do 5 lat 20 punktów;
Ilość lat powyżej 5 lat do 6 lat 30 punktów;
Ilość lat powyżej 6 lat 40 punktów;
Zaoferowanie przez Wykonawcę osoby oddelegowanej do realizacji zamówienia z brakiem kwalifikacji potwierdzonych certyfikatem lub poniżej 3 lat spowoduje odrzucenie oferty, jako treść niezgodna z warunkami zamówienia – art. 226 ust 1 pkt 5 ustawy Pzp. Brak określenia przez Wykonawcę ilości lat posiadania kwalifikacji osoby wyznaczonej do realizacji zamówienia spowoduje odrzucenie oferty, jako treść niezgodna z warunkami zamówienia – art. 226 ust 1 pkt 5 ustawy Pzp.
Łączna ocena ofert:
W = C + K
W – wskaźnik oceny oferty
C – ilość punktów przyznanych ofercie w kryterium Cena;
K – ilość punktów przyznanych ofercie w kryterium Ilość lat posiadania kwalifikacji w branży „IT Security" jednej osoby wyznaczonej do realizacji zamówienia.
Punktacja przyznawana ofertom w poszczególnych kryteriach oceny ofert będzie liczona z dokładnością do dwóch miejsc po przecinku, zgodnie z zasadami arytmetyki.
Maksymalna ilość punktów, jaką może otrzymać oferta wynosi 100 punktów od 1 członka komisji przetargowej. Po dokonaniu oceny ofert punkty przyznane przez każdego z członków komisji przetargowej będą zsumowane dla każdego z kryteriów oddzielnie.
Jeżeli nie można wybrać oferty najkorzystniejszej z uwagi na to, że dwie lub więcej ofert przedstawi taki sam wskaźnik oceny ofert, Zamawiający spośród tych ofert wybierze ofertę z niższą ceną.

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: organizacja, kwalifikacje zawodowe i doświadczenie osób wyznaczonych do realizacji zamówienia

4.3.5.) Nazwa kryterium: Ilość lat posiadania kwalifikacji w branży „IT Security" jednej osoby wyznaczonej do realizacji zamówienia(K)

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 4

5.3.) Warunki udziału w postępowaniu: Tak

5.4.) Nazwa i opis warunków udziału w postępowaniu.
Część I
Zamawiający wymaga, aby Wykonawca dysponował odpowiednim potencjałem oraz osobami zdolnymi do wykonania zamówienia. Zamawiający uzna warunek za spełniony, jeżeli Wykonawca dysponuje co najmniej dwoma specjalistami IT o następujących kompetencjach:
Specjalista 1 ma posiadać kompetencje z zakresu bezpieczeństwa IT i posiadać co najmniej 2 z poniższych certyfikacji branżowych lub równoważnych pod względem zakresu certyfikacji. Wskazane certyfikacje muszą być ważne w chwili składania oferty:
a. EC-Council CEH: Certified Ethical Hacker
b. Cisco CCNP Security/CCIE Security
c. Cisco CCNA CyberOps
d. PCNSE: Palo Alto Networks Certified Network Security Engineer
e. Fortinet Certified Expert (FCX) in Cybersecurity
f. OSCP: Offensive Security Certified Professional
Specjalista 2 ma posiadać kompetencje z zakresu bezpieczeństwa IT i posiadać co najmniej 1 z poniższych certyfikacji branżowych lub równoważnych pod względem zakresu certyfikacji. Wskazane certyfikacje muszą być ważne w chwili składania oferty:
a. EC-Council CEH: Certified Ethical Hacker
b. Cisco CCNP Security/CCIE Security
c. Cisco CCNA CyberOps
d. PCNSE: Palo Alto Networks Certified Network Security Engineer
e. Fortinet Certified Expert (FCX) in Cybersecurity
f. OSCP: Offensive Security Certified Professional
g. LPIC-1 Certified Linux Administrator

Część II
Zamawiający wymaga, aby Wykonawca dysponował odpowiednim potencjałem oraz osobami zdolnymi do wykonania zamówienia. Zamawiający uzna warunek za spełniony, jeżeli Wykonawca dysponuje co najmniej jednym specjalistą posiadającymi uprawnienia na podstawie certyfikatów wskazanych w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999) w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2020 poz. 1369 ze zm.).
Dodatkowo, do wykonania usługi będzie oddelegowanych co najmniej trzech specjalistów. Specjalista 1 musi posiadać kompetencje z zakresu bezpieczeństwa IT i posiadać co najmniej 2 z poniższych certyfikatów branżowych lub certyfikaty równoważne pod względem zakresu certyfikacji. Wskazane certyfikaty muszą być ważne w chwili składania oferty:
a) EC-Council CEH: Certified Ethical Hacker
b) Cisco CCNP Security/CCIE Security
c) Cisco CCNA CyberOps
d) PCNSE: Palo Alto Networks Certified Network Security Engineer
e) Fortinet Certified Expert (FCX) in Cybersecurity
Specjalista 2 musi posiadać kompetencje z zakresu bezpieczeństwa IT i posiadać co najmniej 1 z poniższych certyfikatów branżowych lub certyfikaty równoważne pod względem zakresu certyfikacji. Wskazane certyfikaty muszą być ważne w chwili składania oferty:
a) EC-Council CEH: Certified Ethical Hacker
b) Cisco CCNP Security/CCIE Security
c) Cisco CCNA CyberOps
d) PCNSE: Palo Alto Networks Certified Network Security Engineer
e) Fortinet Certified Expert (FCX) in Cybersecurity
f) LPIC-1 Certified Linux Administrator
Specjalista 3 musi posiadać kompetencje z zakresu bezpieczeństwa IT i posiadać co najmniej 1 z poniższych certyfikatów branżowych lub certyfikaty równoważne pod względem zakresu certyfikacji. Wskazane certyfikaty muszą być ważne w chwili składania oferty:
a) EC-Council CEH: Certified Ethical Hacker
b) Cisco CCNP Security/CCIE Security
c) Cisco CCNA CyberOps
d) PCNSE: Palo Alto Networks Certified Network Security Engineer
e) Fortinet Certified Expert (FCX) in Cybersecurity
f) MCSA: Windows Serwer 2016

Część III
Zamawiający wymaga, aby Wykonawca dysponował odpowiednim potencjałem oraz osobami zdolnymi do wykonania

zamówienia. Zamawiający uzna warunek za spełniony, jeżeli Wykonawca dysponuje jednym Instruktorem o kompetencjach z zakresu bezpieczeństwa IT i posiada co najmniej 2 z poniższych certyfikacji branżowych lub certyfikaty równoważne pod względem zakresu certyfikacji. Wskazane certyfikacje muszą być ważne w chwili składania oferty:
a. EC-Council CEH: Certified Ethical Hacker
b. Cisco CCNP Security/CCIE Security
c. Cisco CCNA CyberOps
d. PCNSE: Palo Alto Networks Certified Network Security Engineer
e. Fortinet Certified Expert (FCX) in Cybersecurity
f. OSCP: Offensive Security Certified Professional

Część IV
Zamawiający wymaga, aby Wykonawca dysponował odpowiednim potencjałem oraz osobami zdolnymi do wykonania zamówienia. Zamawiający uzna warunek za spełniony, jeżeli Wykonawca dysponuje co najmniej dwoma specjalistami IT o następujących kompetencjach:
Specjalista 1 ma posiadać kompetencje z zakresu bezpieczeństwa IT i posiadać co najmniej 2 z poniższych certyfikacji branżowych lub certyfikaty równoważne pod względem zakresu certyfikacji. Wskazane certyfikacje muszą być ważne w chwili składania oferty:
a. EC-Council CEH: Certified Ethical Hacker
b. Cisco CCNP Security/CCIE Security
c. Cisco CCNA CyberOps
d. PCNSE: Palo Alto Networks Certified Network Security Engineer
e. Fortinet Certified Expert (FCX) in Cybersecurity
f. OSCP: Offensive Security Certified Professional
Specjalista 2 ma posiadać kompetencje z zakresu bezpieczeństwa IT i posiadać co najmniej 1 z poniższych certyfikacji branżowych lub certyfikaty równoważne pod względem zakresu certyfikacji. Wskazane certyfikacje muszą być ważne w chwili składania oferty:
a. EC-Council CEH: Certified Ethical Hacker
b. Cisco CCNP Security/CCIE Security
c. Cisco CCNA CyberOps
d. PCNSE: Palo Alto Networks Certified Network Security Engineer
e. Fortinet Certified Expert (FCX) in Cybersecurity
f. OSCP: Offensive Security Certified Professional
g. LPIC-1 Certified Linux Administrator

Wykonawca składa wykaz osób ze wskazaniem posiadanych certyfikatów i ich numerów, z załączeniem dowodów potwierdzających posiadanie certyfikatów. Wzór wykazu osób stanowi załącznik nr 8 do SWZ.

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: Na potwierdzenie braku podstaw wykluczenia:
a) Odpis lub informacja z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 ustawy PZP, sporządzone nie wcześniej niż 3 miesiące przed złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;
W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, dokument składa każdy z Wykonawców wspólnie ubiegających się o zamówienie.
b) Oświadczenie Wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy PZP o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz.U. z 2024 r., poz. 594 z późn. zm), z innym Wykonawcą, który złożył odrębną ofertę, ofertę częściową lub wniosek o dopuszczenie do udziału w postępowaniu, albo oświadczenie o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej lub wniosku o dopuszczenie do udziału w postępowaniu niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej - załącznik nr 3 do SWZ;
W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, dokument składa każdy z Wykonawców wspólnie ubiegających się o zamówienie.

5.7.) Wykaz podmiotowych środków dowodowych na potwierdzenie spełniania warunków udziału w postępowaniu: Na potwierdzenie spełnienia warunków udziału w postępowaniu:
Wykaz osób skierowanych do realizacji zamówienia wraz z dołączonymi certyfikatami potwierdzającymi posiadanie wymaganych kompetencji - załącznik nr 8 do SWZ.

5.8.) Wykaz przedmiotowych środków dowodowych:
Przedmiotowe środki dowodowe:
1) W celu potwierdzenia zgodności z kryteriami określonymi w opisie kryteriów oceny ofert, zgodnie z art. 106 ust. 1 ustawy Pzp, Zamawiający żąda następujących przedmiotowych środków dowodowych, składanych wraz z ofertą:
a) Certyfikat potwierdzający ilość lat posiadania kwalifikacji w branży „IT Security” jednej osoby oddelegowanej do realizacji zamówienia: CEH lub CCNP Security lub CCIE Security lub CCNA CyberOps lub PCNSE lub FCX in Cybersecurity lub równoważny.
2) Przedmiotowe środki dowodowe sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski.

3) Przedmiotowe środki dowodowe pod rygorem nieważności należy złożyć opatrzone kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.

5.9.) Zamawiający przewiduje uzupełnienie przedmiotowych środków dowodowych: Tak

5.10.) Przedmiotowe środki dowodowe podlegające uzupełnieniu po złożeniu oferty:
Jeżeli Wykonawca nie złoży przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe są niekompletne, Zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie (art. 107 ust. 2 ustawy Pzp). Przepisu nie stosuje się, jeżeli przedmiotowy środek dowodowy służy potwierdzeniu zgodności z cechami lub kryteriami określonymi w opisie kryteriów oceny ofert lub, pomimo złożenia przedmiotowego środka dowodowego, oferta podlega odrzuceniu albo zachodzą przesłanki unieważnienia postępowania.

5.11.) Wykaz innych wymaganych oświadczeń lub dokumentów:
1. Formularz ofertowy, stanowiący załącznik nr 1 do SWZ wraz z wypełnionym załącznikiem nr 1a – specyfikacja serwera (dla części I). Do oferty należy dołączyć aktualne dokumenty potwierdzające status prawny wykonawcy, np. odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej. Oferta nie musi zawierać tych dokumentów w przypadku wskazania przez wykonawcę, że są one dostępne w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych. Upoważnienie osób podpisujących ofertę musi bezpośrednio wynikać z ww. dokumentów.
Formularz ofertowy musi ponadto zawierać oświadczenie Wykonawcy w zakresie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO
2. Oświadczenie Podmiotu udostępniającego zasoby na które Wykonawca będzie się powoływał w celu spełniania warunków udziału w postępowaniu stanowiący załącznik nr 5 do SWZ (dołączyć jeżeli dotyczy).
Zgodnie z art. 118 ust 3 ustawy Pzp musi złożyć wraz z ofertą zobowiązania ww. podmiotów do oddania mu do dyspozycji tych zasobów na potrzeby realizacji zamówienia albo inne podmiotowe środki dowodowe potwierdzające, że Wykonawca realizując zamówienia będzie dysponował niezbędnymi zasobami tych podmiotów. Zgodnie z art. 118 ust. 4 ustawy Pzp zobowiązanie podmiotu udostępniającego zasoby, którego wzór stanowi załącznik nr 9 do SWZ, musi potwierdzać, że stosunek łączący wykonawcę
z podmiotami udostepniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz musi określać w szczególności:
a) zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;
b) sposób i okres udostępniania Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
c) czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane lub usługi, których wskazane zdolności dotyczą.
3. Oświadczenie z art. 125 ust 1 ustawy Pzp o braku podstaw do wykluczenia z postępowania o udzielenie zamówienia publicznego oraz o spełnieniu warunków udziału w postępowaniu i art. 7 ust 1 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainie oraz służących ochronie bezpieczeństwa narodowego - załącznik nr 4 do SWZ.
4. Oświadczenie podmiotu udostępniającego zasoby dotyczące przesłanek wykluczenia z art. 7 ust 1 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainie oraz służących ochronie bezpieczeństwa narodowego – załącznik nr 9 do SWZ (dołączyć jeżeli dotyczy).
5. Pełnomocnictwo - jeżeli oferta wraz z oświadczeniami składana jest przez pełnomocnika należy do oferty załączyć pełnomocnictwo do tej czynności (dołączyć jeżeli dotyczy).
6. Pełnomocnictwo dla pełnomocnika – Wykonawcy występujący wspólnie są zobowiązani do ustanowienia pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania ich w postępowaniu i zawarcia umowy w sprawie przedmiotowego zamówienia publicznego (dołączyć jeżeli dotyczy).
7. Oświadczenie wykonawców ubiegających się wspólnie o udzielenie zamówienia, z którego wynika jaki zakres rzeczowy zamówienia realizować zamierzają poszczególni Wykonawcy – załącznik nr 7 do SWZ (dołączyć jeżeli dotyczy).

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:
1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo winno być załączone do oferty.
2. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenia, o których mowa w Rozdziale X SWZ, składa każdy z Wykonawców. Oświadczenia i dokumenty potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w zakresie, w jakim każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu.

3. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają do oferty oświadczenie, z którego wynika, które roboty budowlane wykonają poszczególni wykonawcy.
4. Oświadczenia i dokumenty potwierdzające brak podstaw do wykluczenia z postępowania składa każdy z Wykonawców wspólnie ubiegających się o zamówienie.
5. W odniesieniu do warunków określonych w Rozdziale VIII SWZ, wymagania te muszą być spełnione wspólnie przez Wykonawców składających ofertę w postępowaniu (nie musi spełniać osobno każdy z Wykonawców składających ofertę wspólną). Na ich potwierdzenie należy złożyć dokumenty określone w Rozdziale X SWZ.
6. Jeżeli oferta Wykonawców wspólnie ubiegających się o udzielenie niniejszego zamówienia zostanie wybrana, Wykonawcy zobowiązani są przedłożyć Zamawiającemu przed zawarciem umowy w sprawie niniejszego zamówienia, umowę regulującą swoją współpracę.

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:
Oprócz przypadków, o których mowa w art. 455 ust. 1 pkt 2-4 i ust. 2 ustawy Pzp, Zamawiający przewiduje, na podstawie art. 455 ust. 1 pkt. 1 ustawy Pzp, możliwość dokonywania zmian postanowień niniejszej umowy w następujących przypadkach:
1) wyniknięcia rozbieżności lub niejasności w rozumieniu pojęć użytych w umowie, których nie można usunąć w inny sposób, a zmiana będzie umożliwiać usunięcie rozbieżności i doprecyzowanie umowy w celu jednoznacznej interpretacji jej zapisów przez Strony;
2) jeżeli w trakcie realizacji umowy zaistnieje konieczność dokonania uszczegółowienia, wykładni lub doprecyzowania poszczególnych zapisów umowy, nie powodujących zmiany celu i istoty umowy;
3) gdy niedokonanie zmian w Umowie będzie ewidentnym działaniem sprzecznym z zasadą celowego i oszczędnego gospodarowania środkami publicznym;
4) gdy zaistnieją nieprzewidywalne okoliczności, tzn. okoliczności, których przy zachowaniu należytej staranności nie można było przewidzieć, zmiany będą konieczne, gdyż bez ich dokonania zamówienie nie będzie mogło być zrealizowane, nie będzie mógł zostać osiągnięty cel, dla którego będzie wykonywane;
5) powstania nadzwyczajnych okoliczności (nie będących „siłą wyższą”), grożące rażącą stratą, których strony nie przewidziały przy zawarciu umowy;
6) gdy wystąpią inne, niż przewidziane powyżej, zmiany dotyczące zawartej umowy, które są korzystne dla Zamawiającego i które nie naruszają art. 454 ustawy Pzp.
Wszelkie zmiany i uzupełnienia treści umowy mogą być dokonywane wyłącznie za zgodą obydwu stron i stosownie uzasadnione, w formie pisemnej, pod rygorem nieważności.
Przyjmuje się, że nie stanowią zmiany Umowy następujące zmiany:
1) danych związanych z obsługą administracyjno-organizacyjną Umowy;
2) danych teleadresowych;
3) danych rejestrowych;
4) danych osób wyznaczonych do kontaktów i koordynowania spraw związanych z realizacją.
Pełny zakres przewidywanych zmian umowy znajduje się w załączniku nr 2 do SWZ - projekt umowy.

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

7.6.) Zamawiający przewiduje następujące wymagania związane z realizacją zamówienia:

w zakresie zatrudnienia na podstawie stosunku pracy, w okolicznościach, o których mowa w art. 95 ustawy

SEKCJA VIII – PROCEDURA

8.1.) Termin składania ofert: 2024-10-17 09:00

8.2.) Miejsce składania ofert: https://platformazakupowa.pl/pn/rudniki

8.3.) Termin otwarcia ofert: 2024-10-17 09:05

8.4.) Termin związania ofertą: do 2024-11-15

SEKCJA IX – POZOSTAŁE INFORMACJE

Wynagrodzenie wykonawcy za realizację przedmiotu zamówienia będzie wynagrodzeniem ryczałtowym, nie podlegającym weryfikacji, w konsekwencji czego konieczność wykonania prac, bez których przedmiot zamówienia nie mógłby być zrealizowany, a których Wykonawca wcześniej nie przewidział nie będzie miała wpływu na wysokość wynagrodzenia – nie będzie stanowiła podstaw do podwyższenia ceny określonej w ofercie.

UWAGA: Rozliczenie ryczałtowe. Zakres usług i dostaw do wykonania w ramach niniejszego zamówienia określa załączony opis przedmiotu zamówienia.
Zamawiający stosownie do art. 95 ust 1 ustawy Pzp, określa obowiązek zatrudnienia przez Wykonawcę lub Podwykonawcę na podstawie stosunku pracy osób wykonujących wskazane przez Zamawiającego czynności w zakresie realizacji zamówienia, jeżeli wykonanie tych czynności polega na wykonywaniu pracy w sposób określony w art. 22 § 1 ustawy z 26 czerwca 1974 r – Kodeks pracy (t.j. Dz.U. z 2023 r., poz. 1465 z późn. zm.) – tj. następujące czynności: specjalistów IT świadczących usługi utrzymania środowiska w zakresie części I.
Szczegółowe wymagania dotyczące realizacji oraz egzekwowania wymogu zatrudnienia na podstawie stosunku pracy zostały określone w projektowanych postanowieniach umowy. Projekt umowy stanowi załącznik nr 2 do SWZ.
Wymagany przez Zamawiającego okres gwarancji na przedmiot zamówienia wynosi odpowiednio dla poszczególnych części:
1) Część I – 6 miesięcy
2) Część II – 6 miesięcy
3) Część III – nie dotyczy
4) Część IV – 6 miesięcy
licząc od daty wykonania usług. Szczegółowe informacje dotyczące gwarancji znajdują się w § 10 projektów umów – załącznik nr 2 do SWZ.
Z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp, zgodnie z art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t.j. Dz.U. z 2024, poz. 507) 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 ww. 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 ww. 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 ww. ustawy.
Wykluczenie następuje na okres trwania okoliczności określonych w ust. 3.