



Cyberbezpieczny Samorząd

Znak sprawy : ZP.PP.14.2024

Mszana Dolna, dnia 26.09.2024 r.

Zamawiający: Miasto Mszana Dolna

34-730 Mszana Dolna

ul. marsz. Józefa Piłsudskiego 2

Zapytanie Ofertowe

Dotyczy: Projektu pn. „Cyberbezpieczne Miasto Mszana Dolna” dofinansowanego w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

POSTANOWIENIA OGÓLNE

Do udzielenia przedmiotowego zamówienia nie stosuje się przepisów Ustawy z dnia 11 września 2019 r.- Prawo zamówień publicznych.

Niniejsze postępowanie prowadzone jest w oparciu o Regulamin udzielania zamówień publicznych, których wartość nie przekracza kwoty 130 000,00 zł netto obowiązujący w Urzędzie Miasta Mszana Dolna, wprowadzony Zarządzeniem nr 19/2021 Burmistrza Miasta Mszana Dolna z dnia 26.02.2021r., zmieniony Zarządzeniem nr 49/2021 Burmistrza Miasta Mszana Dolna z dnia 28.04.2021r., Zarządzeniem nr 115/2022 Burmistrza Miasta Mszana Dolna z dnia 14.11.2022r. oraz Zarządzeniem nr 119/2023 Burmistrza Miasta Mszana Dolna z dnia 29.12.2023r.

Procedura postępowania będzie prowadzona zgodnie z Wytycznymi dotyczącymi kwalifikowalności wydatków na lata 2021-2027 i dokumentami wydanymi na podstawie art. 6 ust. 2 ustawy wdrożeniowej.

TERMIN I SPOSÓB SKŁADANIA OFERT ORAZ ZAŁĄCZNIKÓW DO ZAPYTANIA.

Oferty stanowiące odpowiedź na niniejsze Zapytanie ofertowe należy złożyć na załączonym formularzu oferty (załącznik nr 1a lub 1b do zapytania ofertowego) bezpośrednio poprzez Bazę Konkurencyjności BK 2021.

Do formularza oferty należy załączyć załączniki nr 3, 4, 5, 6 do zapytania ofertowego.

Wykonawca, który nie złoży w/w dokumentów z ofertą, zostanie wezwany o jego uzupełnienie.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

Bieg terminu składania ofert rozpoczyna się dnia następującego po dniu upublicznienia zapytania ofertowego, a kończy się z upływem ostatniego dnia (zastosowanie ma art. 115 Kodeksu cywilnego). O terminowym złożeniu oferty decyduje data złożenia oferty za pośrednictwem BK2021.

Część: 1 Usługi doradztwa merytorycznego oraz doradztwa technicznego

Oferty wariantowe i częściowe w ramach części 1 nie są dopuszczalne.

I. PRZEDMIOTY ZAMÓWIENIA DLA CZĘŚCI 1 Typ: Usługa Podkategoria: Usługi IT

Przedmiot zamówienia obejmuje realizację na rzecz Zamawiającego usług wsparcia merytorycznego oraz doradztwa technicznego w zakresie realizacji projektu pn. „Cyberbezpieczne Miasto Mszana Dolna”, uwzględniającym zapisy aktualnego regulaminu konkursu grantowego pn. "Cyberbezpieczny Samorząd", dostępnego na stronie: <https://www.gov.pl/web/cppc/cyberbezpieczny-samorząd>.

Zadanie 1. Doradztwo techniczne obejmuje przygotowanie dokumentacji technicznej, przygotowanie koncepcji realizacji projektu obejmującej następujący zakres:

1. Aktualizacja dokumentacji SZBI wraz z niezbędnymi komponentami:
 - 1) Audyt wstępny i konsultacje określające poziom cyberbezpieczeństwa w tym audyt dokumentacyjny na podst. KRI wykazujący posiadanie wymaganej dokumentacji w tym zakresie , tj. procedury, polityki, itp. oraz audyt podatności na wzór zał. Nr 8 CG KRI dla Urzędu Miasta (dalej „UM”), Miejskiego Ośrodka Pomocy Społecznej (dalej „MOPS”) i Centrum Usług Wspólnych (dalej „CUW”).
 - 2) Aktualizacja dokumentacji SZBI dla UM, MOPS, CUW w tym: PBI, Polityka ODO, Polityka ZSI, Polityka zarządzania ciągłością działania, Procedury zarządzania incydentami cyberbezpieczeństwa, Analizy Ryzyka SZBI, Przygotowanie dokumentacji zgodnie z wymogami ustawy o KSC.
 - 3) Audyt Bezpieczeństwa Informacji zgodny z przepisami Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności dla UM, MOPS i CUW.
 - 4) Doradztwo w zakresie ustawy o Krajowym Systemie Cyberbezpieczeństwa dla UM, MOPS i CUW.
2. Certyfikowane szkolenia dla kadry kierowniczej oraz pracowników (w tym pracowników IT):
 - 1) Certyfikowane szkolenie z obsługi urządzeń klasy UTM oraz szkolenie stacjonarne dla personelu IT Urzędu Miasta.
 - 2) Certyfikowane szkolenie z obsługi systemu do backupu danych oraz szkolenie stacjonarne dla personelu IT Urzędu Miasta.
 - 3) Symulator zagrożeń UM, MOPS, CUW.
 - 4) Szkolenie z zakresu cyberbezpieczeństwa dedykowane kadrze kierowniczej UM, MOPS i CUW - stacjonarne
 - 5) Szkolenie z zakresu cyberbezpieczeństwa dedykowane pracownikom UM, MOPS i CUW - stacjonarne
3. Dostawy z obszaru technicznego – Zakup sprzętu IT oraz wartości niematerialnych i prawnych.
 - 1) Centralny System Bezpieczeństwa - Oprogramowanie klasy SIEM z elementami XDR Extended Detection and Response, EDR Endpoint Detection and Response, oraz monitoringiem infrastruktury IT
 - 2) Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych
 - 3) UTM - UM, MOPS, CUW - 3 szt.
 - 4) Rozbudowa macierzy o dyski twarde - UM
 - 5) UPS – UM



Cyberbezpieczny Samorząd

Zadanie 2. Usługi wsparcia merytorycznego:

Realizacja usług będzie polegała w szczególności na:

- pomocy przy badaniu zgodności oferty z dokumentacją techniczną i opisem potrzeb Zamawiającego przygotowanych w ramach zadania 1.
- doradztwie podczas realizacji umowy wyłonionego Wykonawcy, w tym ewentualnych kontroli,
- opracowanie procedury monitorowania utrzymania efektów Projektu Grantowego.

Kody CPV

72000000-5 Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia

72600000-6 Usługi doradcze i dodatkowe w zakresie sprzętu komputerowego

72700000-7 Usługi w zakresie sieci komputerowej

79140000-7 Doradztwo prawne i usługi informacyjne

85312320-8 Usługi doradztwa

II. HARMONOGRAM

Etap 1: (Zadanie 1) Początek realizacji: 2024-10-15 Koniec realizacji: 2024-11-30 Występuje płatność częściowa.

Etap 2: (Zadanie 2) Początek realizacji: 2024-10-15 Koniec realizacji: 2026-06-20 Występują płatności częściowe.

III. WARUNKI, JAKIE MUSI SPEŁNIAĆ OFERENT

Podstawowe warunki udziału

1. Zamawiający udziela zamówienia w częściach, z których każda stanowi przedmiot odrębnego postępowania.
2. Możliwe jest składanie ofert częściowych, ofertę można składać na 2 części.
3. Zamawiający nie ogranicza liczby części zamówienia, którą można udzielić jednemu wykonawcy.
4. Zamawiający nie wymaga wniesienia wadium ani zabezpieczenia należytego wykonania umowy.
5. Rozliczenia między Zamawiającym, a Wykonawcą będą prowadzone w złotych polskich (PLN).
6. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
7. Postępowanie jest prowadzone w języku polskim. Zamawiający nie dopuszcza złożenia ofert w innym języku.
8. Wykonawca ma prawo złożyć tylko jedną ofertę na każdą z części.
9. Zamawiający nie przewiduje udzielenia zaliczek na poczet wykonania zamówienia.
10. Zamawiający zastrzega sobie możliwość unieważnienia postępowania bez podania przyczyny.

Dodatkowe warunki udziału

1. Zakaz powiązań osobowych i kapitałowych.

Konflikt interesów oznacza każdą sytuację, w której osoby biorące udział w przygotowaniu lub prowadzeniu postępowania o udzielenie zamówienia lub mogące wpłynąć na wynik tego postępowania mają, bezpośrednio lub pośrednio, interes finansowy, ekonomiczny lub inny interes osobisty, który postrzegać można jako zagrażający ich bezstronności i niezależności w związku z postępowaniem o udzielenie zamówienia.

W celu uniknięcia konfliktu interesów, zamówienia nie mogą być udzielane podmiotom powiązanym z nim osobowo lub kapitałowo.

2. Brak podstaw do wykluczenia.

W związku z zapisami art. 5k ust. 1 Rozporządzenia Rady Unii Europejskiej nr 2022/576 z dnia 8 kwietnia 2022 r. w sprawie zmiany Rozporządzenia (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczącego środków ograniczających



Cyberbezpieczny Samorząd

w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 111 z 8.4.2022, str. 1), zwane dalej Rozporządzeniem (UE) oraz z zapisami art. 7 ust.1 ustawy z dnia 13 kwietnia 2022r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2022r. poz.835) Wykonawca składa oświadczenie dotyczące braku podstaw do wykluczenia.

Lista wymaganych dokumentów/oświadczeń

1. Oświadczenie Wykonawcy o braku powiązań.
2. Oświadczenie Wykonawcy o braku podstaw do wykluczenia.
3. Potwierdzenie doświadczenia: Referencje wraz z opisem realizowanych projektów lub inne dokumenty poświadczające wykonanie usług doradczych.
4. Wykaz osób, skierowanych przez Wykonawcę do realizacji zamówienia publicznego wraz z certyfikatami.

Wiedza i doświadczenie

Wykonawca posiada co najmniej dwuletnie doświadczenie zawodowe oraz odpowiednią wiedzę w prowadzeniu i wdrażaniu projektów z zakresu cyberbezpieczeństwa.

Akceptowalne są kwalifikacje zawodowe nadane przez Centrum Certyfikacji Kompetencji i Potwierdzania Kwalifikacji Polskiego Towarzystwa Informatycznego lub równoważne oraz certyfikaty poparte stosownym doświadczeniem. Akceptowalne certyfikaty to w szczególności audytor wewnętrzny i zewnętrzny normy PN_ISO/IEC 27001, CISA, CIA oraz równoważne poświadczenia/certyfikaty z zakresu cyberbezpieczeństwa.

Przez doświadczenie zawodowe rozumie się realizację projektów z zakresu cyberbezpieczeństwa przez okres co najmniej dwóch lat.

Doświadczenie należy udokumentować poprzez wykaz usług wraz z opisami wcześniejszych projektów (zrealizowanych i zakończonych projektów) potwierdzonych referencjami, przy czym nie jest istotne czy doświadczenie jest ciągłe czy nie.

Osoby zdolne do wykonania zamówienia

Wykonawca dysponuje co najmniej dwoma osobami/specjalistami posiadającymi co najmniej dwuletnie doświadczenie zawodowe oraz odpowiednią wiedzę w prowadzeniu i wdrażaniu projektów z zakresu cyberbezpieczeństwa. Każda z tych osób powinna posiadać co najmniej 1 certyfikat.

Akceptowalne certyfikaty to w szczególności audytor wewnętrzny i zewnętrzny normy PN_ISO/IEC 27001, CISA, CIA oraz równoważne poświadczenia/certyfikaty z zakresu cyberbezpieczeństwa, wskazane w ROZPORZĄDZENIU MINISTRA CYFRYZACJI z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu, lub w ROZPORZĄDZENIU RADY MINISTRÓW z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa lub równoważne poświadczenia/certyfikaty z zakresu cyberbezpieczeństwa.

Kryteria oceny do części 1

Obowiązuje kryterium cenowe.

Wybór najkorzystniejszej oferty nastąpi w oparciu o kryterium: najniższa cena -100% cena

Część: 2 Specjalistyczne wsparcie IT w zakresie cyberbezpieczeństwa

Oferty wariantowe nie są dopuszczalne

I. **PRZEDMIOTY ZAMÓWIENIA DLA CZĘŚCI 2** Typ: Usługa Podkategoria: Usługi IT



Cyberbezpieczny Samorząd

Specjalistyczne wsparcie IT w zakresie cyberbezpieczeństwa w wymiarze 8h stacjonarnie w wyznaczony 1 dzień w miesiącu oraz 30h online w ciągu miesiąca (przy czym nie wykorzystane godziny nie przechodzą na następny miesiąc). Wsparcie będzie realizowane od dnia podpisania umowy do 20.06.2026r.

W zakresie usług specjalistycznego wsparcia informatycznego Zamawiający zdiagnozował konkretne obszary za które będzie odpowiadał Wykonawca: wsparcie wdrożenia reguł zgodności z przepisami prawnymi oraz standardami bezpieczeństwa, konfiguracji i zarządzania firewallami, IDS /IPS i innymi mechanizmami obronnymi, zarządzanie dostępem i autoryzacją użytkowników, wsparcie monitoringu sieci i alarmowania w czasie rzeczywistym, wdrożenia reguł dla backupu i archiwizacji danych, szyfrowania danych wrażliwych, zabezpieczenia przed złośliwym oprogramowaniem (wsparcie konfiguracji antywirus i antymalware), wsparcie implementacji planu reagowania na incydenty bezpieczeństwa, wspomaganie analizy po incydentach i rekomendacje, wsparcie monitorowania logów i zdarzeń związanych z bezpieczeństwem oraz sporządzania okresowych raportów dotyczących stanu bezpieczeństwa.

Kody CPV

72000000-5 Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia

72600000-6 Usługi doradcze i dodatkowe w zakresie sprzętu komputerowego

72700000-7 Usługi w zakresie sieci komputerowej

79140000-7 Doradztwo prawne i usługi informacyjne

85312320-8 Usługi doradztwa

II. HARMONOGRAM

Początek realizacji: 2024-10-15 Koniec realizacji: 2026-06-20 Występują płatności częściowe.

III. WARUNKI, JAKIE MUSI SPEŁNIAĆ OFERENT

Podstawowe warunki udziału

1. Zamawiający udziela zamówienia w częściach, z których każda stanowi przedmiot odrębnego postępowania.
2. Możliwe jest składanie ofert częściowych, ofertę można składać na 2 części.
3. Zamawiający nie ogranicza liczby części zamówienia, którą można udzielić jednemu wykonawcy.
4. Zamawiający nie wymaga wniesienia wadium ani zabezpieczenia należytego wykonania umowy.
5. Rozliczenia między Zamawiającym, a Wykonawcą będą prowadzone w złotych polskich (PLN).
6. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
7. Postępowanie jest prowadzone w języku polskim. Zamawiający nie dopuszcza złożenia ofert w innym języku.
8. Wykonawca ma prawo złożyć tylko jedną ofertę na każdą z części.
9. Zamawiający nie przewiduje udzielenia zaliczek na poczet wykonania zamówienia.
10. Zamawiający zastrzega sobie możliwość unieważnienia postępowania bez podania przyczyny.

Dodatkowe warunki udziału

1. Zakaz powiązań osobowych i kapitałowych.

Konflikt interesów oznacza każdą sytuację, w której osoby biorące udział w przygotowaniu lub prowadzeniu postępowania o udzielenie zamówienia lub mogące wpłynąć na wynik tego postępowania mają, bezpośrednio lub pośrednio, interes finansowy, ekonomiczny lub inny interes osobisty, który postrzegać można jako zagrażający ich bezstronności i niezależności w związku z postępowaniem o udzielenie zamówienia.

W celu uniknięcia konfliktu interesów, zamówienia nie mogą być udzielane podmiotom powiązanym z nim osobowo lub kapitałowo.

2. Brak podstaw do wykluczenia.



Cyberbezpieczny Samorząd

W związku z zapisami art. 5k ust. 1 Rozporządzenia Rady Unii Europejskiej nr 2022/576 z dnia 8 kwietnia 2022 r. w sprawie zmiany Rozporządzenia (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 111 z 8.4.2022, str. 1), zwane dalej Rozporządzeniem (UE) oraz z zapisami art. 7 ust.1 ustawy z dnia 13 kwietnia 2022r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2022r. poz.835) Wykonawca składa oświadczenie dotyczące braku podstaw do wykluczenia.

Lista wymaganych dokumentów/oświadczeń

1. Oświadczenie Wykonawcy o braku powiązań.
2. Oświadczenie Wykonawcy o braku podstaw do wykluczenia.
3. Potwierdzenie doświadczenia: Referencje wraz z opisem realizowanych projektów lub inne dokumenty poświadczające wykonanie usług doradczych.
4. Wykaz osób, skierowanych przez Wykonawcę do realizacji zamówienia publicznego wraz z certyfikatami.

Wiedza i doświadczenie

Wykonawca posiada co najmniej dwuletnie doświadczenie zawodowe oraz odpowiednią wiedzę w prowadzeniu i wdrażaniu projektów z zakresu cyberbezpieczeństwa.

Akceptowalne są kwalifikacje zawodowe nadane przez Centrum Certyfikacji Kompetencji i Potwierdzania Kwalifikacji Polskiego Towarzystwa Informatycznego lub równoważne oraz certyfikaty poparte stosownym doświadczeniem. Akceptowalne certyfikaty to w szczególności audytor wewnętrzny i zewnętrzny normy PN_ISO/IEC 27001, CISA, CIA oraz równoważne poświadczenia/certyfikaty z zakresu cyberbezpieczeństwa.

Przez doświadczenie zawodowe rozumie się realizację projektów z zakresu cyberbezpieczeństwa przez okres co najmniej dwóch lat.

Doświadczenie należy udokumentować poprzez wykaz usług wraz z opisami wcześniejszych projektów (zrealizowanych i zakończonych projektów) potwierdzonych referencjami, przy czym nie jest istotne czy doświadczenie jest ciągłe czy nie.

Osoby zdolne do wykonania zamówienia

Wykonawca dysponuje co najmniej dwoma osobami/specjalistami posiadającymi co najmniej dwuletnie doświadczenie zawodowe oraz odpowiednią wiedzę w prowadzeniu i wdrażaniu projektów z zakresu cyberbezpieczeństwa. Każda z tych osób powinna posiadać co najmniej 1 certyfikat.

Akceptowalne certyfikaty to w szczególności audytor wewnętrzny i zewnętrzny normy PN_ISO/IEC 27001, CISA, CIA oraz równoważne poświadczenia/certyfikaty z zakresu cyberbezpieczeństwa, wskazane w ROZPORZĄDZENIU MINISTRA CYFRYZACJI z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu, lub w ROZPORZĄDZENIU RADY MINISTRÓW z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa lub równoważne poświadczenia/certyfikaty z zakresu cyberbezpieczeństwa.

Kryteria oceny do części 2

Obowiązuje kryterium cenowe.

Wybór najkorzystniejszej oferty nastąpi w oparciu o kryterium: najniższa cena -100% cena

ZATWIERDZAM:

Burmistrz Miasta
mgr Agnieszka Orzeł
(podpis elektroniczny)