Zapytanie ofertowe na udzielenie zamówienia publicznego

Zamówienie finansowane ze środków Unii Europejskiej w ramach konkursu grantowego „Cyberbezpieczny Samorząd" realizowanego w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe. Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Nazwa i adres Zamawiającego

Gmina Stara Dąbrowa
Stara Dąbrowa 20,
73-112 Stara Dąbrowa
NIP 8542229275 Regon 811685728
Numer telefonu: 915739820

Adres e-mail: ug@staradabrowa.pl

Tryb udzielenia zamówienia

Do niniejszego postępowania nie stosuje się przepisów ustawy z dnia 11 września 2019 roku Prawo zamówień Publicznych (Dz. U. 2024, poz. 1320 z późn. zm.)

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest:

1) **Opracowanie wraz z wdrożeniem dokumentacji SZBI dla Urzędu Gminy w Starej Dąbrowie.**
2) **Przeprowadzenie Audytu Krajowych Ram Interoperacyjności jako wymóg końcowego rozliczenia projektu.**
3) **Przeprowadzenie testów socjotechnicznych.**

Szczegółowy opis przedmiotu zamówienia:

ZADANIE NUMER 1

Opracowanie wraz z wdrożeniem dokumentacji SZBI dla Urzędu Gminy w Starej Dąbrowie.

W ramach realizowanego przedmiotu zamówienia Wykonawca jest zobowiązany do aktualizacji dokumentacji z zakresu bezpieczeństwa informacji posiadanej przez Zamawiającego oraz opracowania i wdrożenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

Szczegółowy opis przedmiotu zamówienia obejmuje czynności związanych z wdrożeniem dokumentacji systemu zarządzania bezpieczeństwem informacji, zgodnego z poniższymi wymaganiami:

a) rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
b) ustawa z dnia z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa wraz z nowelizacjami ustawy, które zostaną dokonane w czasie realizacji zamówienia;
c) rozporządzenie 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 ochronie danych);
d) wymagania norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005 i w oparciu o główne założenia norm ISO 31000 w zakresie zarządzania ryzykiem oraz PN-EN ISO 22301 w zakresie ciągłości działania;
e) wymagania regulaminu konkursu grantowego oraz umowy o powierzenie grantu zawartej w ramach projektu „Cyberbezpieczny Samorząd".

Szczegółowy zakres dokumentacji powinien składać się z następujących obszarów:

a) zarządzanie aktywami,
b) zarządzanie ryzykiem,
c) zapewnienie bezpieczeństwa systemów informatycznych oraz ich rozwoju,
d) zapewnienie bezpieczeństwa fizycznego,
e) kontrola dostępu do oprogramowania i infrastruktury sieciowej,
f) klasyfikacja informacji oraz nadzoru nad dokumentacją,
g) zapewnienie bezpieczeństwa zasobów ludzkich,
h) wykonywanie kopii zapasowych,
i) stosowanie kryptografii,
j) obsługa incydentów i realizacja działań korygujących,
k) prowadzenie wewnętrznych audytów bezpieczeństwa,
l) prowadzenie przeglądów zarządzania,
m) zapewnienie ciągłości działania i przywracania normalnej działalności po wystąpieniu zakłóceń,
n) zapewnienie bezpieczeństwa łańcucha dostaw,
o) postępowanie z podatnościami systemów i sieci,
p) Deklaracja stosowania (w oparciu o załącznik A do normy ISO/IEC 27001:2022).

W ramach wdrażania Systemu Zarządzania Bezpieczeństwem Informacji powinny zostać uregulowane zabezpieczenia określone w załączniku A do normy ISO/IEC 27001:2022.

ZADANIE NUMER 2

Przeprowadzenie Audytu Krajowych Ram Interoperacyjności jako wymóg końcowego rozliczenia projektu.

W ramach realizowanego przedmiotu zamówienia Wykonawca jest zobowiązany do zapewnienia:

a) Realizacji audytu bezpieczeństwa informacji w siedzibie Zamawiającego (nie jest przewidziana zdalna realizacja);
b) Wypełnienie ankiety dojrzałości z zakresu cyberbezpieczeństwa, zgodnej z regulaminem projektu „Cyberbezpieczny Samorząd" dla urzędu oraz wszystkich jednostek objętych projektem;
c) Zapewnienia zgodności realizowanego audytu bezpieczeństwa informacji z następującymi wymaganiami:
    i. Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych- Ustawy o Krajowym Systemie Cyberbezpieczeństwa;
    ii. Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
    iii. wymagań określonych w normie ISO 27001.
d) Opracowanie raportu z audytu wraz z rekomendacjami do wdrożenia w ramach projektu „Cyberbezpieczny Samorząd", w szczególności w odniesieniu do wyników ankiety wypełnionej przez Zamawiającego, zgodnie z regulaminem projektu „Cyberbezpieczny Samorząd".

Szczegółowy zakres audytu powinien objąć następujące obszary:

a) prawidłowości prowadzonej przez Zamawiającego dokumentacji aktualnej oraz planowanej, dotyczącej Systemu Zarządzania Bezpieczeństwa Informacji w zakresie jego poufności, dostępności i integralności informacji,
b) zapewniania przez Zamawiającego aktualizacji regulacji wewnętrznych w zakresie, dotyczącym zmieniającego się otoczenia,

c) utrzymywania przez Zamawiającego aktualności inwentaryzacji sprzętu i oprogramowania, służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację,

d) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy,

e) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji,

f) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji z uwzględnieniem aspektów związanych z bezpieczeństwem informacji,

g) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,

h) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,

i) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie,

j) ustalonych zapisów zawieranych w umowach serwisowych gwarantujących odpowiedni poziom bezpieczeństwa informacji,

k) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych,

l) zapewnienia odpowiedniego określonego przez KRI poziomu bezpieczeństwa w systemach teleinformatycznych,

m) sposobu postępowania z incydentami związanymi z bezpieczeństwem informacji, w tym bezzwłocznego zgłaszania takich incydentów,

n) przeglądu zgodności przetwarzania danych osobowych z obowiązującymi przepisami prawa,

o) przeglądu istniejących regulacji wewnętrznych odnośnie bezpieczeństwa przetwarzania danych osobowych,

p) przeglądu aktualnie wykorzystywanych dokumentów mających związek z ochroną danych osobowych,
q) weryfikacji istniejących procedur zarządzania systemami teleinformatycznymi,
r) weryfikacji ochrony przed oprogramowaniem szkodliwym,
s) weryfikacji procedur zarządzania kopiami zapasowymi,
t) weryfikacji procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania,
u) weryfikacji zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe,
v) weryfikacji haseł,
w) analizy i oceny mechanizmów zarządzania aktualizacjami.

W ramach audytu powinna zostać wykonana analiza techniczna (obejmująca odrębny raport) w zakresie monitorowania sieci internetowej urzędu wraz z wydaniem zaleceń i rekomendacji w zakresie wdrożenia systemów SOC. Analiza powinna zostać opracowania bezpośrednio przez osoby wskazane w ofercie i posiadające uprawnienia w zakresie wymaganych certyfikatów.

Wymagany zakres opracowania:

- Identyfikacja kluczowych elementów infrastruktury teleinformatycznej Urzędu, obejmującej urządzenia sieciowe, serwery, stacje robocze, systemy operacyjne, usługi sieciowe oraz wykorzystywane rozwiązania bezpieczeństwa.
- Przygotowanie metodyki prowadzenia monitoringu obejmującej zakres monitorowanych zasobów, źródła logów, sposób pozyskiwania danych oraz kryteria oceny zdarzeń bezpieczeństwa.
- Ocena kompletności logów generowanych przez urządzenia sieciowe, systemy operacyjne, aplikacje oraz rozwiązania zabezpieczające, wraz z identyfikacją obszarów wymagających uzupełnienia.
- Weryfikacja aktualnie stosowanych mechanizmów bezpieczeństwa, obejmujących m.in. zapory sieciowe, systemy wykrywania i zapobiegania włamaniom, ochronę punktów końcowych, systemy uwierzytelniania oraz rozwiązania do zarządzania tożsamością.

- Analiza zidentyfikowanych zdarzeń oraz konfiguracji infrastruktury pod kątem występowania podatności technicznych.
- Analiza istniejących procedur monitorowania, wykrywania i obsługi incydentów bezpieczeństwa, z uwzględnieniem obowiązujących regulacji wewnętrznych oraz dobrych praktyk wynikających z norm i standardów bezpieczeństwa informacji.
- Określenie stopnia przygotowania infrastruktury oraz procesów organizacyjnych do wdrożenia usług Security Operations Center, ze wskazaniem braków technicznych, organizacyjnych i proceduralnych.
- Przygotowanie szczegółowych rekomendacji obejmujących:
    - proponowany model funkcjonowania SOC (wewnętrzny, zewnętrzny lub hybrydowy),
    - zakres monitorowanych systemów,
    - wymagane źródła logów,
    - rekomendowaną architekturę rozwiązania,
    - niezbędne działania organizacyjne i techniczne poprzedzające wdrożenie,
    - priorytety wdrożeniowe oraz harmonogram realizacji.
    - opracowanie listy działań mających na celu podniesienie poziomu cyberbezpieczeństwa, usunięcie zidentyfikowanych niezgodności oraz zwiększenie skuteczności monitorowania i reagowania na incydenty.
- Wykonawca sporządzi raport końcowy zawierający co najmniej:
    - charakterystykę analizowanego środowiska teleinformatycznego,
    - zestawienie potencjalnych zagrożeń,
    - ocenę aktualnego poziomu bezpieczeństwa infrastruktury,
    - analizę gotowości do wdrożenia rozwiązania klasy SOC,
    - rekomendacje techniczne, organizacyjne i proceduralne,
    - podsumowanie oraz wnioski końcowe.

Raport końcowy powinien zostać przekazany w formie elektronicznej (format PDF oraz edytowalny DOCX) i stanowić kompletną dokumentację z przeprowadzonych prac. Dokument powinien zawierać jednoznaczne wnioski oraz rekomendacje umożliwiające Zamawiającemu podjęcie decyzji dotyczącej wdrożenia rozwiązania klasy Security

Operations Center (SOC), zgodnie z najlepszymi praktykami w zakresie cyberbezpieczeństwa oraz obowiązującymi standardami.

ZADANIE NR 3

Przeprowadzenie testów socjotechnicznych.

Szczegółowy opis przedmiotu zamówienia obejmuje czynności związanych z realizacją zadania zgodnego z poniższymi wymaganiami:

1. W ramach wykonywanych prac Wykonawca przeprowadzi kompleksową weryfikację wiedzy z zakresu przestrzegania zasad bezpieczeństwa informacji poprzez wykonanie testu socjotechnicznego.
2. Wykonawca wspólnie z Zamawiający ustali szczegółowy scenariusz testu socjotechnicznego, który będzie odpowiadał na aktualne problemy związane z pracą Zamawiającego lub sytuacją społeczno – gospodarczą.
3. Wykonawca przeprowadzi test socjotechniczny z dedykowanego adresu mailowego opartego na specjalnie założonej stronie internetowej pozwalającej na uwiarygodnienie wiadomości.
4. Wykonawca zaprojektuje minimum jeden szablon wiadomości mailowej, która będzie wysyłana z dedykowanej strony internetowej.
5. Zamawiający przekaże Wykonawcy adresy mailowe pracowników objętych testem.
6. Wykonawca przeprowadzi wysyłkę wiadomości mailowych, przyjmując odpowiedni podział pracowników.
7. W trakcie realizacji testu Wykonawca będzie odpowiedzialny za monitorowanie reakcji pracowników, analizowanie odpowiedzi i interakcji odbiorców z wysłanymi wiadomościami, a także wprowadzanie zmian w realizowanej kampanii, w celu zapewnienia efektywności testu.
8. Wykonawca przeanalizuje wyniki testów oraz na tej podstawie opracuje raport, który zostanie przekazany Zamawiającemu, a następnie będzie stanowił podstawę do odpowiedniej analizy tematyki szkoleń i zostanie przedstawiony pracownikom podczas szkoleń.

Wymagany termin wykonania zamówienia: **18 września 2026 roku**.

Warunki udziału w postępowaniu

O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy nie podlegają wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspierania agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. 2024 r., poz. 507), zgodnie z którym z postępowania o udzielenie zamówienia publicznego wyklucza się:

1) wykonawcę wymienionego w wykazach określonych w rozporządzeniu Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy zwanym dalej „rozporządzeniem 765/2006" i rozporządzeniu Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających zwanym dalej „rozporządzeniem 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, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2023 r. poz. 1124, 1285, 1723 i 1843) 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, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, 295 i 1598) 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."

Wykluczenie następuje na okres trwania okoliczności określonych wyżej wymienionych ppkt.

W przypadku wykonawców występujących wspólnie, każdy z wykonawców nie może podlegać wykluczeniu z postępowania.

W postępowaniu nie może brać udziału wykonawca powiązany osobowo lub kapitałowo z Zamawiającym. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między beneficjentem lub osobami upoważnionymi do zaciągania zobowiązań w imieniu beneficjenta lub osobami wykonującymi w imieniu beneficjenta czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy a wykonawcą, polegające w szczególności na:

a) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej, posiadaniu co najmniej 10% udziałów lub akcji (o ile niższy próg nie wynika

z przepisów prawa), pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,

b) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia, lub związaniu z tytułu przysposobienia, opieki lub kurateli albo pozostawaniu we wspólnym pożyciu z wykonawcą, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych wykonawców ubiegających się o udzielenie zamówienia,

c) pozostawaniu z Wykonawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.

W celu potwierdzenia braku wykluczenia, wykonawca składa oświadczenie stanowiące załącznik nr 3 do zapytania ofertowego.

W celu wzięcia udziału w postępowaniu Wykonawca wykaże, że jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności, związanej z przedmiotem zamówienia, na kwotę nie niższą niż 100.000,00 złotych (słownie: sto tysięcy złotych).

O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy posiadają dwuletnie doświadczenie w przedmiocie zamówienia i przekażą wraz z ofertą referencje/protokoły odbioru w zakresie realizacji trzech tożsamych zleceń, potencjał techniczny i osobowy niezbędny do wykonania zamówienia oraz dysponują min. 2 osobami posiadającymi uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa. Wykaz certyfikatów wskazanych w w/w rozporządzeniu:

1) Certified Internal Auditor (CIA);

2) Certified Information System Auditor (CISA);

3) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;

4) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia

13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;

5) Certified Information Security Manager (CISM);

6) Certified in Risk and Information Systems Control (CRISC);

7) Certified in the Governance of Enterprise IT (CGEIT);

8) Certified Information Systems Security Professional (CISSP);

9) Systems Security Certified Practitioner (SSCP);

10) Certified Reliability Professional;

11) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

W zakresie potencjału technicznego, w związku z wykonywaniem analizy technicznej infrastruktury Zamawiającego wymagane jest dysponowanie zespołem, w którym osoby będą posiadały następujące uprawnienia: CompTIA Security+ lub CompTIA CySa+ lub Certified Ethical Hacker (CEH).

Wykonawca powinien posiadać również certyfikat ISO 27001 wydany przez niezależną i akredytowaną jednostkę, obejmujący obszar działania firmy, który odpowiada zakresowi realizowanych działań.

Na potwierdzenie spełnienia ww. warunku, Wykonawca przekaże Zamawiającemu certyfikat uprawniający do przeprowadzenia audytu dla osoby skierowanej do realizacji przedmiotu zamówienia w momencie wyboru oferty Wykonawcy.

Oferta podlega odrzuceniu jeżeli wykonawca nie potwierdzi, że spełnia warunki udziału w postępowaniu.

Kryteria oceny ofert

Ocenie podlegają jedynie oferty niepodlegające odrzuceniu.

Zamawiający dokona wyboru oferty najkorzystniejszej na podstawie następujących kryteriów oceny ofert:

l.p.	nazwa kryterium	waga
1.	cena oferty	100

Cena oferty (C)

Ocenie podlega wskazana w formularzu oferty cena oferty wraz z podatkiem VAT. Oferty zostaną ocenione według wzoru:

$$\text{Ilość uzyskanych punktów} = \frac{\text{cena najniższa spośród badanych ofert}}{\text{cena badanej oferty}} \times 100$$

a. Najkorzystniejsza oferta może otrzymać maksymalnie 100 punktów.

b. Jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że zostały złożone oferty o takiej samej cenie, zamawiający wzywa wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez zamawiającego ofert dodatkowych. Wykonawcy składając oferty dodatkowe nie mogą zaoferować cen wyższych niż zaoferowane w pierwotnie złożonych ofertach.

Cenę oferty należy obliczyć uwzględniając wszystkie koszty niezbędne do wykonania przedmiotu zamówienia.

Cena oferty winna być wyrażona w złotych (PLN) i ewentualnie dodatkowo w groszach, z dokładnością do dwóch miejsc po przecinku.

W ofercie należy podać cenę netto, wartość podatku VAT oraz cenę brutto za realizację przedmiotu zamówienia. Cena brutto stanowi cenę oferty.

Przygotowanie oraz złożenie oferty

Wykonawca może złożyć tylko jedna ofertę. Złożenie więcej niż jednej oferty spowoduje odrzucenie wszystkich ofert złożonych przez wykonawcę.

Ofertę należy sporządzić w języku polskim. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.

Ofertę należy sporządzić poprzez wypełnienie formularza oferty, którego wzór stanowi załącznik nr 1 do zapytania ofertowego. Wraz z formularzem oferty należy złożyć następujące dokumenty:

i. oświadczenie wykonawcy o niepodleganiu wykluczeniu z postępowania, sporządzone zgodnie z wzorem stanowiącym załącznik nr 3 do zapytania ofertowego,

ii. pełnomocnictwo w przypadku, gdy ofertę podpisuje osoba nieuprawniona na podstawie dokumentów rejestrowych podmiotu do reprezentowania wykonawcy.

Formularz oferty wraz z wymaganym oświadczeniem należy złożyć w formie elektronicznej tj. opatrzonej kwalifikowanym podpisem elektronicznym lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym osoby uprawnionej do reprezentowania wykonawcy zgodnie z zasadami reprezentacji wskazanymi we właściwym rejestrze lub ustanowionego pełnomocnika. Brak podpisu oferty w wyżej wymieniony sposób będzie skutkował odrzuceniem oferty.

Termin składania ofert upływa w dniu 18 sierpnia 2026 r. o godz. 10:00.

Złożenie oferty wraz z załącznikami następuje poprzez wysłanie oferty na adres e-mail ug@staradabrowa.pl w terminie ustalonym powyżej.

Oferty złożone po terminie zostaną odrzucone przez zamawiającego.

Otwarcie ofert nastąpi niezwłocznie po upływie terminu na ich złożenie.

Ocena ofert

Zamawiający dokona weryfikacji oferty pod kątem spełniania wymogów określonych w niniejszym zapytaniu ofertowym, w szczególności w zakresie dotyczącym sposobu i formy złożenia oferty oraz spełniania warunków udziału w postępowaniu.

Zamawiający poprawi w ofercie oczywiste omyłki pisarskie oraz oczywiste omyłki rachunkowe z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek, niezwłocznie zawiadamiając o tym wykonawcę, którego oferta została poprawiona.

Jeżeli wykonawca nie złożył oświadczenia o braku podstaw do wykluczenia z niniejszego postępowania lub dokumentów składanych na potwierdzenie spełniania warunków udziału lub pełnomocnictwa lub są one niekompletne lub zawierają błędy, zamawiający wzywa wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w wyznaczonym terminie, chyba że:

1) oferta wykonawcy podlegają odrzuceniu bez względu na ich złożenie, uzupełnienie lub poprawienie lub

2) zachodzą przesłanki unieważnienia postępowania.

W toku badania ofert zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych ofert i dokumentów, w szczególności dokumentów potwierdzających spełnianie warunków udziału w niniejszym postępowaniu.

Oferta zostanie odrzucona jeśli:

3) została złożona po upływie terminu składania ofert,

4) została złożona w sposób niezgodny z zapytaniem ofertowym,

5) nie została podpisana przez osobę uprawnioną do reprezentowania wykonawcy lub wykonawca nie złożył wymaganego pełnomocnictwa,

6) została złożona przez wykonawcę, który nie wykazał, że spełnia warunki udziału określone w niniejszym zapytaniu ofertowym w wyznaczonym terminie,

7) wykonawca złożył wymagane od wykonawcy oświadczenia i dokumenty w formie i w sposób niezgodny z postanowieniami zapytania ofertowego,

8) złożone oświadczenia lub dokumenty zawierają nieprawdziwe informacje, które mają lub mogą mieć wpływ na decyzję o wyborze oferty najkorzystniejszej,

9) wykonawca nie udzielił w wyznaczonym terminie wyjaśnień dotyczących ceny lub jeżeli złożone przez wykonawcę wyjaśnienia wraz z dowodami nie uzasadniają podanej w ofercie ceny.

Nieodrzucone oferty zostaną ocenione według kryteriów oceny ofert.

Zamawiający udzieli zamówienia wykonawcy, którego oferta spełnia wymagania określone w niniejszym zapytaniu ofertowym i uzyskała największą liczbę punktów.

Zamawiający niezwłocznie zawiadomi wybranego wykonawcę o miejscu i terminie zawarcia umowy. Wykonawca jest zobowiązany do zawarcia umowy na warunkach określonych w projekcie umowy stanowiącym załącznik do zapytania ofertowego.

W przypadku gdy wybrany wykonawca odstąpi od zawarcia umowy w sprawie zamówienia, zamawiający może zawrzeć umowę z wykonawcą, który w przeprowadzonym postępowaniu o udzielenie zamówienia uzyskał kolejną najwyższą liczbę punktów.

W toku oceny i badania ofert Zamawiający zastrzega sobie prawo żądać od wykonawców wyjaśnień lub uzupełnień dotyczących treści złożonych ofert i załączonych dokumentów.

Wykonawca jest związany ofertą przez okres 30 dni kalendarzowych liczonych od dnia upływu terminu na złożenie ofert.

Zamawiający ma prawo unieważnienia postępowania na każdym etapie bez podawania przyczyny.

Klauzula informacyjna

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 ochronie danych, zwane dalej „RODO") (Dz. U. UE. L. 119.1 z 04.05.2016) informuję, iż:
Administratorem danych osobowych jest Gmina Stara Dąbrowa z siedzibą w Starej Dąbrowie (73-112) Stara Dąbrowa 20 . Z administratorem można skontaktować się mailowo: ug@staradabrowa.pl lub pisemnie na adres siedziby administratora;
Administrator wyznaczył inspektora ochrony danych, z którym można się skontaktować mailowo: iod@staradabrowa.pl . Z inspektorem ochrony danych można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych;
Zgodnie z treścią art. 6 ust. 1 lit. c RODO dane osobowe przetwarzane będą w celu realizacji procesu wyboru wykonawcy na podstawie prowadzonego postępowania o udzielenie zamówienia publicznego, a następnie realizacji postanowień umownych związanych z wykonywanym zamówieniem;

W związku z przetwarzaniem danych osobowych w celach wskazanych powyżej, dane osobowe mogą być udostępniane innym odbiorcom lub kategoriom odbiorców danych osobowych, na podstawie przepisów prawa oraz zawartych umów powierzenia przetwarzania danych, jeżeli wymagane byłoby to w celu realizacji postanowień umownych,
Dane osobowe będą przetwarzane przez okres niezbędny do realizacji wskazanych powyżej celów przetwarzania, w tym również obowiązku archiwizacyjnego wynikającego z przepisów prawa;
Posiada Pani/Pan prawo do:
10) żądania od administratora dostępu do treści swoich danych osobowych, prawo do ich sprostowania oraz ograniczenia przetwarzania (z zastrzeżeniem przypadku, o którym mowa w art. 18 ust. 2 RODO, kiedy to nieograniczone przetwarzanie danych przez Administratora odnosi się do ich 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),
11) wniesienia skargi do organu nadzorczego,
Nie przysługuje Panu/Pani prawo do:
12) usunięcia lub przenoszenia danych osobowych,
13) wniesienia sprzeciwu wobec przetwarzania danych osobowych;
Podanie danych osobowych jest konieczne w celu realizacji postępowania o udzielenie zamówienia publicznego oraz realizacji postanowień umownych. Niepodanie danych będzie skutkowało brakiem możliwości rozpatrzenia oferty złożonej w postępowaniu oraz zawarcia umowy.

Załączniki

W ramach prowadzonego postępowania opublikowane zostają następujące załączniki:
Załącznik numer 1 – Projekt umowy
Załącznik numer 2 - Oświadczenie o braku podstaw do wykluczenia z postępowania
Załącznik numer 3 – Formularz oferty
Załącznik numer 4 – Klauzula informacyjna FERC

WÓJT
Tomasz Ogonowski