RGT.ZP.58.2024 Miłakowo, dnia 15.10.2024 r.

Zapytanie ofertowe

p.n. „**Zwiększenie poziomu cyberbezpieczeństwa w Gminie Miłakowo**” **– część I**

Tryb udzielania zamówienia: Niniejsze postępowanie toczy się w oparciu o zasadę konkurencyjności określoną w aktualnie obowiązujących Wytycznych w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu na Rozwój Cyfrowy, Europejskiego Funduszu Rozwoju Regionalnego oraz Regulaminu udzielenia zamówień publicznych przez Gminę Miłakowo o wartości nieprzekraczającej kwoty 130 000 złotych netto (Zarządzenie nr 1/2021 Burmistrza Miłakowa z dnia 04.01.2021r.)

I. Zamawiający:

Gmina Miłakowo, ul. Olsztyńska 16, 14-310 Miłakowo, NIP 741-20-25-674.

II. Opis przedmiotu zamówienia:

1. Zamówienie realizowane jest w ramach Projektu grantowego „Zwiększenie poziomu cyberbezpieczeństwa w Gminie Miłakowo”
2. Przedmiotem zamówienia jest:
   1) przeprowadzenie audytu wstępnego zgodnie z KRI UoKSC RODO
   2) opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) i Ciągłości Działania wraz z doradztwem w obszarze wdrożenia.
   3) szkolenia stacjonarne pracowników z zakresu cyberbezpieczeństwa;
   4) przeprowadzenie audytu końcowego.

   w ramach Projektu Cyberbezpieczny Samorząd, współfinansowanego przez Unię Europejską.
3. Szczegółowy opis zakresu zamówienia:
   1) **Audyt** - Zamawiający zleca przeprowadzenie audytu wstępnego i końcowego oraz konsultacji określających poziom cyberbezpieczeństwa w obszarze organizacyjnym – Urząd Miejski w Miłakowie. W zakresie Audytu mają znaleźć się:
      a) weryfikacja zgodności przyjętych procedur z przepisami 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 (t. j. Dz. U. 2024 r., poz. 773);
      b) weryfikacja zgodności przyjętych procedur z zakresu cyberbezpieczeństwa wynikających z obowiązków określonych w przepisach Ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. z 2023 r., poz. 913,);
      c) weryfikacja zgodności przyjętych procedur z przepisami z zakresu ochrony danych wynikających z obowiązków określonych w przepisach 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 Dz. U. UE. L. 2016, poz. 119.1 i 2. – dalej „RODO”) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. z 2019 r., poz. 1781);

d) omówienie wyników Audytu wstępnego oraz wydanie rekomendacji Zamawiającemu.
e) omówienie wyników Audytu końcowego.

2) **Opracowanie dokumentacji SZBI** - przedmiot zamówienia obejmuje następujące etapy realizacji usługi:

Etap I: „Polityka Bezpieczeństwa Informacji jako podstawowy element systemu zarządzania bezpieczeństwem informacji" obejmuje następujące czynności:

a) analiza ekspercka wyników zrealizowanego uprzednio na zasobach Zamawiającego audytu wstępnego systemu bezpieczeństwa informacji w ww. obszarze;
b) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Bezpieczeństwa Informacji realizowane w formie on-line
c) przygotowanie i przekazanie Polityki Bezpieczeństwa Informacji;
d) doradztwo we wdrożeniu Polityki Bezpieczeństwa Informacji i bieżące wsparcie ekspertów przez czas trwania Umowy;
e) przeprowadzenie szkolenia w formie e-learningowej dla całego personelu Zamawiającego w obszarze przyjętej Polityki Bezpieczeństwa Informacji.

Etap II: „Polityka Zarządzania Systemem Teleinformatycznym" obejmuje następujące czynności:

a) analiza ekspercka wyników zrealizowanego uprzednio na zasobach Zamawiającego audytu wstępnego systemu bezpieczeństwa informacji w ww. obszarze;
b) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Zarządzania Systemem Informatycznym realizowane w formie on-line;
c) przygotowanie i przekazanie Polityki Zarządzania Systemem Informatycznym wraz z Planami Ciągłości Działania w obszarze IT;
d) doradztwo we wdrożeniu Polityki Zarządzania Systemem Informatycznym i bieżące wsparcie ekspertów przez czas trwania Umowy;
e) przeprowadzenie szkolenia w formie e-learningowej dla całego personelu Zamawiającego obejmujące wszystkie procesy z obszaru Krajowych Ram Interoperacyjności.

Etap III: „Polityka Zarządzania Ciągłością Działania wraz z Planami Ciągłości Działania w obszarze IT" obejmuje następujące czynności:

a) analiza ekspercka wyników zrealizowanego uprzednio na zasobach Zamawiającego audytu wstępnego systemu bezpieczeństwa informacji w ww. obszarze;
b) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Zarządzania Ciągłością Działania realizowane w formie on-line
c) przygotowanie i przekazanie Polityki Zarządzania Ciągłością Działania wraz z Planami Ciągłości Działania w obszarze IT;
d) doradztwo we wdrożeniu Polityki Zarządzania Ciągłością Działania i bieżące wsparcie ekspertów przez czas trwania Umowy;
e) przeprowadzenie szkolenia w formie e-learningowej dla całego personelu Zamawiającego obejmujące obszar utrzymania ciągłości działania.

Etap IV: „Polityka Zarządzania Incydentami Cyberbezpieczeństwa" obejmuje następujące czynności:

a) analiza ekspercka wyników zrealizowanego uprzednio na zasobach Zamawiającego audytu wstępnego systemu bezpieczeństwa informacji w ww. obszarze;
b) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Zarządzania Incydentami Cyberbezpieczeństwa realizowane w formie on-line
c) przygotowanie i przekazanie Polityki Zarządzania Incydentami Cyberbezpieczeństwa;
d) przygotowanie i przekazanie Planu Reagowania na Incydenty;
e) przygotowanie i przekazanie Planu Zarządzania Podatnościami;
f) doradztwo we wdrożeniu dokumentacji wymienionej w ppkt c)-e) i bieżące wsparcie ekspertów przez czas trwania Umowy;

g) przeprowadzenie szkolenia w formie e-learningowej dla całego personelu Zamawiającego obejmujące wdrożoną Politykę Zarządzania Incydentami Cyberbezpieczeństwa oraz wymogów prawnych wynikających Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. z 2023 r., poz. 913).

Etap V: „Polityka Ochrony Danych" obejmuje następujące czynności:

a) analiza ekspercka wyników zrealizowanego uprzednio na zasobach Zamawiającego audytu wstępnego systemu bezpieczeństwa informacji w ww. obszarze;
b) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Ochrony Danych realizowane w formie on-line
c) przygotowanie i przekazanie Polityki Ochrony Danych;
d) doradztwo we wdrożeniu Polityki Ochrony Danych i bieżące wsparcie ekspertów przez czas trwania Umowy;
e) przeprowadzenie szkolenia w formie e-learningowej dla całego personelu Zamawiającego obejmujące wdrożoną Politykę Ochrony Danych oraz omówienie przyjętych procedur zgodnie z przepisami z zakresu ochrony danych w oparciu o przepisy 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) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. z 2019 r., poz. 1781).

Etap VI: „Analiza Ryzyka Bezpieczeństwa Informacji" obejmuje następujące czynności:

a) analiza ekspercka wyników zrealizowanego uprzednio na zasobach Zamawiającego audytu wstępnego systemu bezpieczeństwa informacji w ww. obszarze;
b) konsultacje z przedstawicielem Zamawiającego w celu przeprowadzenia analizy ryzyka realizowane w formie on-line
c) przygotowanie i przekazanie Raportu z przeprowadzonej analizy ryzyka wraz z omówieniem obszarów o podniesionym ryzyku wraz z rekomendacjami ekspertów.

Etap VII: W ramach realizowanej usługi, ponad czynności o których mowa w pkt 1-6, zostaną przygotowane przez Wykonawcę lub dostosowane w przypadku ich posiadania przez Zamawiającego, następujące dokumenty:

a) procedury korzystania z urządzeń mobilnych,
b) procedury pracy zdalnej,
c) postępowanie z nośnikami,
d) procedury kontroli dostępu,
e) zabezpieczenie pomieszczeń i obiektów,
f) procedury czystego biurka,
g) procedury czystego ekranu,
h) procedury kopii zapasowych,
i) procedury ochrony logów,
j) bezpieczeństwo komunikacji,
k) zarządzanie bezpieczeństwem sieci,
l) przesyłanie informacji,
m) plany ciągłości działania,
n) procedury zarządzania incydentami,
o) prywatność i ochrona danych osobowych,
p) szacowanie ryzyka w obszarze bezpieczeństwa informacji,
q) szkolenia personelu,
r) plan zarządzania podatnościami,

s) plan reagowania na incydenty,
t) plan przywracania.

3) **Szkolenia stacjonarne pracowników z zakresu cyberbezpieczeństwa**.

- Szkolenia maja obejmować swoim zakresem następujące zagadnienia:

a) Data Leak – czym jest i jakie zagrożenia niesie.
b) Polityka haseł – praktyczne podejście i narzędzia wspomagające.
c) Socjotechniki – podstawowe definicje i przykłady użycia.
d) Phishing / Spoofing – nigdy nie wiesz kto jest po drugiej stronie.
e) Vhishing / ID Call Hijacking – telefony też nie są w pełni bezpieczne.
f) Metadane – czyli dane o danych.
g) Web Archive – Internet nie zapomina.
h) Pliki Cookies – czym są popularne „ciasteczka".
i) Zagrożenia związane z nieznanym sprzętem – jak nieznany pendrive może zaszkodzić całej instytucji.
j) Ataki Bruteforce / Ataki Słownikowe – podstawowe metody łamania haseł.
k) Spear Phishing – wszystko co „powiesz" (w sieci) może zostać użyte przeciwko Tobie.

- Sposób organizacji szkolenia:

a) Tryb wykonania szkolenia: stacjonarne
b) Czas trwania szkolenia: 2 godziny
c) Liczba pracowników do przeszkolenia: 25 osób
d) Ilość grup szkoleniowych: 2
e) Liczba dni szkoleniowych: 2 dni
f) Termin wykonania szkoleń: Jedno szkolenie w terminie do 15 grudnia 2024 i jedno szkolenie w terminie do 30 czerwca 2025.

- Zamawiający żąda, aby osoby nieobecne na szkoleniu stacjonarnym miały zapewniony dostęp do szkolenia w wersji online.

4. Zamawiający nie dopuszcza składania ofert częściowych z uwagi na potrzebę skoordynowania wyników działań poszczególnych części zamówienia. Wyniki przeprowadzonego audytu muszą przełożyć się na wytyczne do stworzenia dokumentacji SZBI oraz przeprowadzanych szkoleń. Podział zamówienia na części mógłby zagrozić właściwemu wykonaniu zamówienia.

5. Kody dotyczące przedmiotu zamówienia określone we Wspólnym Słowniku Zamówień:

79212200-5 Usługi audytu wewnętrznego.
80500000-9 Usługi szkoleniowe
72220000-3 Usługi doradcę w zakresie systemów i doradztwo techniczne
72225000-8 Usługi w zakresie oceny i analizy gwarancji jakości systemu

III. Termin realizacji umowy:

Całość zamówienia ma zostać wykonana w terminie do **15.04.2026** r.

IV. Kryteria oceny oferty:

1. Oceny ofert będzie dokonywał Zamawiający. Zamawiający może żądać udzielania przez Wykonawców wyjaśnień dotyczących treści złożonych ofert oraz dokonać poprawek oczywistych pomyłek w treści oferty, niezwłocznie zawiadamiając o tym wykonawcę.

2. Przy wyborze oferty Zamawiający będzie kierował się kryteriami oceny ofert, o których mowa w ust. 3.

3. W odniesieniu do wykonawców, którzy spełnili przedstawione warunki, Zamawiający dokona oceny ofert na podstawie następujących kryteriów:

1) Cena (C) - 100 %

4. Kryterium „Cena" (C) - (waga 100%) - liczba punktów, które można uzyskać w przedmiotowym kryterium zostanie obliczona wg następującego wzoru: $C=(C_{min}: C_{oferty})$ x 100 pkt, gdzie:

C - oznacza punkty za cenę brutto za wykonanie całości przedmiotu zamówienia,

C_{min} - oznacza najniższą cenę spośród złożonych ofert,

C_{oferty} - oznacza cenę badanej oferty

V. Wykluczenia - informacja na temat zakazu powiązań osobowych lub kapitałowych:

1. W postępowaniu nie mogą brać udziału podmioty, które powiązane są z zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu zamawiającego lub osobami wykonującymi w imieniu beneficjenta czynności związane z przygotowaniem przeprowadzeniem procedury wyboru wykonawcy osobowo lub kapitałowo, w szczególności poprzez:
   1) uczestnictwo w spółce, jako wspólnik spółki cywilnej lub spółki osobowej;
   2) posiadanie co najmniej 10 % udziałów lub akcji;
   3) pełnienie funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;
   4) pozostawanie w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia lub w stosunku przysposobienia, opieki lub kurateli.

2. Ocena spełniania warunku nastąpi na podstawie wypełnionego przez Wykonawcę załącznika nr 2 do zapytania ofertowego.

VI. Warunki udziału w postępowaniu.

1. O udzielenie zamówienia mogą ubiegać się wykonawcy, zatrudniający co najmniej trzech pracowników posiadających uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz.1999 z dnia 2018.10.18) w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Potwierdzeniem spełnienia warunku posiadania ww. uprawnień będzie złożenie wraz z ofertą skanu oryginału certyfikatu uprawniającego do przeprowadzenia audytu. Wykaz certyfikatów poniżej:

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

2. Wykonawca w okresie ostatnich trzech lat przed upływem terminu składania ofert (a jeżeli okres prowadzenia działalności jest krótszy w tym okresie), należycie zrealizował co najmniej 5 zamówień polegających na przeprowadzeniu audytu bezpieczeństwa informacji, zgodnie z wymaganiami zawartymi w Krajowych Ramach Interoperacyjności w jednostkach samorządu terytorialnego. Aby potwierdzić spełnienie powyższego warunku należy przesłać odpowiednie referencje lub inne dokumenty wskazujące na realizację takiego zadania. Zamawiający zastrzega sobie możliwość sprawdzenia informacji zawartych w przesłanej dokumentacji.
3. Wykonawca w okresie ostatnich dwóch lat przed upływem terminu składania ofert (a jeżeli okres prowadzenia działalności jest krótszy w tym okresie), należycie zrealizował co najmniej 5 zamówień polegających na opracowaniu dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w jednostkach samorządu terytorialnego. Aby potwierdzić spełnienie powyższego warunku należy przesłać odpowiednie referencje lub inne dokumenty wskazujące na realizację takiego zadania. Zamawiający zastrzega sobie możliwość sprawdzenia informacji zawartych w przesłanej dokumentacji. Wykonawcy, którzy nie wykażą spełnienia warunków udziału w postępowaniu podlegać będą wykluczeniu z udziału w postępowaniu.
4. Wykonawcy, którzy nie wykażą spełnienia warunków udziału w postępowaniu podlegać będą wykluczeniu z udziału w postępowaniu.

VII. Informacje o sposobie porozumiewania się Zamawiającego z Wykonawcami.

1. Pytania dotyczące niniejszego zapytania ofertowego należy składać poprzez odpowiednią zakładkę w bazie konkurencyjności. Zamawiający zastrzega sobie, że może nie udzielić odpowiedzi, jeżeli pytanie wpłynie w okresie krótszym niż 2 dni robocze poprzedzające ostateczny dzień składania ofert. Pytania złożone po godzinie 15:00 będą traktowane jako wpływające z datą dnia następnego.
2. W toku badania i oceny ofert zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych ofert oraz przedmiotowych środków dowodowych lub innych składanych dokumentów lub oświadczeń (jeżeli nie naruszy to konkurencyjności) dotyczących treści złożonych przez nich Ofert z wyłączeniem pozycji z kryterium oceny.

   a) Wezwanie do uzupełnienia przedmiotowych środków dowodowych może być zastosowane jednokrotnie.

   b) Wezwanie do poprawy złożonej oferty może obejmować tylko te dane, które nie powodują odrzucenia oferty pierwotnie złożonej i zostanie wysłane drogą emailową.

VIII. Sposób przygotowania oferty:

1. Ofertę, należy złożyć w języku polskim, sporządzoną pod rygorem nieważności, w formie elektronicznej zachowania elektronicznej formy czynności prawnej wystarcza złożenie oświadczenia woli w postaci elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym) lub postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym przez osoby upoważnione do składania oświadczeń woli w imieniu Wykonawcy zgodnie z formą reprezentacji Wykonawcy określoną w rejestrze lub innym dokumencie, właściwym dla danej formy organizacyjnej Wykonawcy albo przez upełnomocnionego przedstawiciela Wykonawcy, w ogólnie dostępnych formatach danych:

1) Zamawiający zwraca uwagę na ograniczenia wielkości plików podpisywanych profilem zaufanym, który wynosi max IOMB, oraz na ograniczenie wielkości plików podpisywanych w aplikacji eDoApp służącej do składania podpisu osobistego, który wynosi max 5MB,
2) ze względu na niskie ryzyko naruszenia integralności pliku oraz łatwiejszą weryfikację podpisu, Zamawiający zaleca, w miarę możliwości, przekonwertowanie plików składających się na ofertę na format .pdfi opatrzenie ich podpisem kwalifikowanym PAdES,
3) Zamawiający zaleca, aby w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju. Podpisywanie różnymi rodzajami podpisów np. osobistym i kwalifikowanym może doprowadzić do problemów w weryfikacji plików,
4) Zamawiający zaleca, aby Wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty,

5) ofertę należy przygotować z należytą starannością dla podmiotu ubiegającego się o udzielenie zamówienia publicznego i zachowaniem odpowiedniego odstępu czasu do zakończenia przyjmowania ofert. Zaleca się, aby założyć profil Wykonawcy i rozpocząć składanie oferty z odpowiednim wyprzedzeniem,

6) podczas podpisywania plików zaleca się stosowanie algorytmu skrótu SHA2 zamiast SHAI,

7) jeśli wykonawca pakuje dokumenty np. w plik ZIP zalecanej jest wcześniejsze podpisanie każdego ze skompresowanych plików,

8) Zamawiający zaleca wykorzystanie podpisu z kwalifikowanym znacznikiem czasu,

9) Zamawiający zaleca, aby nie wprowadzać jakichkolwiek zmian w plikach po podpisaniu ich podpisem kwalifikowanym. Może to skutkować naruszeniem integralności plików co równoważne będzie z koniecznością odrzucenia oferty w postępowaniu,

2. Każdy Wykonawca może złożyć tylko jedną ofertę i zaproponować tylko jedną cenę. Złożenie więcej niż jednej oferty na realizację przedmiotu zamówienia spowoduje odrzucenie wszystkich ofert złożonych przez Wykonawcę.
3. <u>Oferta musi zawierać następujące oświadczenia i dokumenty</u>:
    1) Wypełniony i podpisany formularz ofertowy zgodnie z załącznikiem nr l ;
    2) Oświadczenie o braku podstaw do wykluczenia – zgodnie z złącznikiem nr 2
    3) Oświadczenie RODO – zgodnie z załącznikiem nr 3 do zapytania;
    4) Wykaz osób posiadających uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu wraz ze skanem oryginału certyfikatów uprawniających do przeprowadzenia audytu — stanowiący załącznik nr 6 do zapytania;
    5) Wypełniony i podpisany wykaz usług w zakresie wykonania audytu bezpieczeństwa informacji — stanowiący załącznik nr 4 do zapytania. Do wykazu należy przedłożyć dowody (referencje/poświadczenia lub inne dokumenty) potwierdzające, że usługi te zostały wykonane w sposób należyty.
    6) Wypełniony i podpisany wykaz usług polegających na opracowaniu dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w jednostkach samorządu terytorialnego w zakresie wykonania audytu bezpieczeństwa informacji — stanowiący załącznik nr 5 do zapytania. Do wykazu należy przedłożyć dowody (referencje/poświadczenia lub inne dokumenty) potwierdzające, że usługi te zostały wykonane w sposób należyty.
    7) pełnomocnictwo - w przypadku ustanowienia przez Wykonawcę pełnomocnika. Wykonawca do oferty dołącza oryginał udzielonego pełnomocnictwa lub notarialnie potwierdzoną jego kopię. Z treści pełnomocnictwa musi jednoznacznie wynikać zakres

umocowania do czynności związanych z postępowaniem o udzielenie zamówienia, w szczególności do podpisania oferty lub do podpisania oferty i podpisania umowy;

4. Jeżeli wykonawca nie złożył dokumentów składanych w postępowaniu lub są one niekompletne lub zawierają błędy, zamawiający wzywa wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w wyznaczonym terminie.
5. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

IX. Termin i miejsce składania ofert:

1. Oferty należy składać poprzez Bazę Konkurencyjności: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/
2. Do złożenia oferty przez Bazę Konkurencyjności konieczne jest założenie konta.
3. Termin składania ofert upływa **24.10.2024 r. do godz. 08:00.**
4. Otwarcie ofert odbędzie się **24.10.2024 r. o godz. 08:05**.
5. W przypadku wystąpienia awarii systemu teleinformatycznego, która spowoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.
6. W przypadku zaistnienia okoliczności, o których mowa w ust. 5 Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postepowania.
7. Otwarcie ofert odbywa się bez udziału wykonawców.

X. Warunki istotnych zmian umowy zawartej w wyniku przeprowadzonego postępowania o udzielenie zamówienia:

1. Zmiana postanowień niniejszej umowy może nastąpić za zgodą obydwu stron wyrażoną na piśmie, w formie aneksu do umowy z zachowaniem formy pisemnej pod rygorem nieważności takiej zmiany.
2. Zamawiający określa następujące okoliczności, które mogą powodować konieczność wprowadzenia zmian w treści zawartej umowy w stosunku do treści złożonej oferty:

   1) wystąpienia okoliczności, których nie można było przewidzieć pomimo zachowania należytej staranności.

   2) zmiany terminu realizacji umowy w przypadku zawieszenia realizacji przedmiotu zamówienia przez zamawiającego,

   3) zmiany terminu realizacji umowy w przypadku wystąpienia przestojów i opóźnień zawinionych przez Zamawiającego,

   4) zamiany terminu realizacji umowy w przypadku działania siły wyższej (np. klęski żywiołowe, strajki), mającej bezpośredni wpływ na terminowość wykonania przedmiotu umowy,

5) zmiany terminu na skutek działań osób trzecich lub organów władzy publicznej, które spowodują przerwanie lub czasowe zawieszenie realizacji przedmiotu umowy,

6) wystąpienia oczywistych omyłek pisarskich i rachunkowych w treści umowy,

3. W przypadkach wystąpienia okoliczności określonych w ust.1 pkt.2)-5) strony ustalą nowe terminy realizacji, z tym, że minimalny okres przesunięcia terminu zakończenia równy będzie okresowi przerwy lub postoju.

Burmistrz Miłakowa

/-/ Krzysztof Szulborski