**ZAPYTANIE OFERTOWE
dla zamówienia publicznego o wartości nieprzekraczającej 130 000,00 złotych**

Postępowanie nie jest objęte przepisami ustawy Prawo zamówień publicznych zgodnie z art. 2 ust. 1 pkt 1 Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 ze zm.).

Postępowanie o udzielenie zamówienia publicznego jest prowadzone zgodnie z obowiązującym w Urzędzie Miejskim w Mrągowie Regulaminem udzielania zamówień publicznych, stanowiącym załącznik nr 1 do Zarządzenia Nr 2/2021 Burmistrza Miasta Mrągowo z dnia 04 stycznia 2021 r. w sprawie: ustalenia Regulaminu udzielania zamówienia publicznych o wartości nieprzekraczającej kwoty wskazanej w art. 2 ust. 1 pkt 1 ustawy Prawo Zamówień Publicznych

Treść niniejszego ogłoszenia nie stanowi oferty w rozumieniu art. 66 i 71 Kodeksu Cywilnego (Dz.U.2020 poz. 1740 ze zm.) t.j. - Ustawa z dnia 23 kwietnia 1964 r.).

Burmistrz Miasta Mrągowo zaprasza do składania ofert na wykonanie:

Usługi audytu i diagnozy cyberbezpieczeństwa Urzędu Miejskiego w Mrągowie stanowiącej przedmiot Umowy o powierzenie grantu o numerze 3583/2/2022 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00. Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego.

1. **ZAMAWIAJĄCY**

Gmina Miasto Mrągowo, ul. Królewiecka 60 A, 11-700 Mrągowo, tel.: 89 741 90 00, Godziny urzędowania: pn. 8:00 – 16:00 wt. – pt. 7:30 – 15:30.

1. **OPIS PRZEDMIOTU ZAMÓWIENIA**

Usługa przeprowadzenie audytu i diagnozy cyberbezpieczeństwa w ramach projektu „Cyfrowa Gmina” w Urzędzie Miejskim w Mrągowie, w dokumentacji projektu określanego jako „diagnoza cyberbezpieczeństwa”, zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina, zakończonego raportem.

Szczegółowy zakres przedmiotu zamówienia:

1. Przeprowadzenie audytu cyberbezpieczeństwa w jednostce Zamawiającego na wszystkich posiadanych przez Zamawiającego urządzeniach przeznaczonych do pracy biurowej oraz audytu sieci teletechnicznej.
2. Parametry zamówienia:
3. ilość serwerów fizycznych: 3
4. ilość serwerów wirtualnych: 15
5. liczba lokalizacji: 2
6. ilość stacji komputerowych: 85
7. Diagnoza zgodności cyberbezpieczeństwa musi uwzględniać:
8. rozporządzenie o Krajowych Ramach Interoperacyjności rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych,
9. ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
10. standard COBIT oraz normę PN-ISO/IEC 27001.
11. Przedstawienie raportu lub innego dokumentu z przeprowadzonej analizy w formie papierowej i elektronicznej;
12. Przekazanie wypełnionego załącznika nr 8 do Regulaminy konkursu Cyfrowa Gmina – Formularza informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa (Formularz stanowi załącznik do niniejszego zapytania).
13. **WSPÓLNY SŁOWNIK ZAMÓWIEŃ:**

**72810000-1 Usługi audytu komputerowego**

1. **WARUNKI UDZIAŁU W POSTĘPOWANIU**
2. Audyt musi zostać przeprowadzony przez osobę posiadająca uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018.1999 z dnia 2018.10.18) w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

**Wykaz certyfikatów wskazanych w w/w rozporządzeniu znajduje się 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.

Potwierdzeniem spełnienia warunku posiadania ww. uprawnień będzie złożenie wraz z ofertą kopii certyfikatu potwierdzonej za zgodność z oryginałem, a w przypadku złożenia oferty drogą elektroniczną przesłanie skanu oryginału podpisanego podpisem kwalifikowanym.

1. Wykonawca powinien posiadać odpowiednią wiedzę i doświadczenie w przeprowadzaniu audytu bezpieczeństwa informacji. 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 2 zamówienia polegające na przeprowadzeniu audytu bezpieczeństwa informacji, zgodnie z wymaganiami zawartymi w Krajowe Ramy Interoperacyjności. Aby potwierdzić spełnienie powyższego warunku należy wypełnić oświadczenie zawarte w Formularzu ofertowym. Zamawiający zastrzega sobie możliwość sprawdzenia informacji zawartych w oświadczeniu poprzez wezwanie do przedstawienia dokumentów potwierdzających spełnienie niniejszego warunku. Wykonawcy, którzy nie wykażą spełnienia warunków udziału w postępowaniu podlegać będą wykluczeniu z udziału w postępowaniu. Ofertę wykonawcy wykluczonego uznaje się za odrzuconą.
2. **OPIS PRZYGOTOWANIA OFERTY**
3. **Kompletny, wypełniony Formularz ofertowy stanowiący załącznik nr 1.**
4. **Oświadczenie o spełnieniu warunków udziału w postępowaniu stanowiące załącznik nr 2.**
5. **Dokumenty potwierdzające wymagane kwalifikacje do przeprowadzenia audytu.**
6. **Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.**
7. **TERMIN ZWIĄZANY OFERTĄ**
8. **Wykonawca pozostaje związany złożoną ofertą przez okres 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.**
9. **Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą.**
10. **TERMIN REALIZACJI**

Wykonawca jest zobowiązany wykonać zamówienie nie później niż w terminie 4 tygodni od dnia zawarcia umowy.

1. **OCENA OFERTY**
2. Przy wyborze oferty do realizacji zamawiający będzie się kierował kryterium: Cena – 100%.
3. Cenę za wykonanie zamówienia należy podać w Formularzu ofertowym – załącznik nr 1.
4. Zaoferowana cena powinna być określona wartością brutto.
5. Cena winna obejmować wszelkie koszty niezbędne do zrealizowania zamówienia.
6. Wykonawca sporządzając ofertę powinien przewidzieć wszelkie okoliczności mogące mieć wpływ na cenę.
7. **UWAGI**

**Ofertę cenową należy:**

1. **złożyć** w siedzibie Zamawiającego:

Urząd Miejski w Mrągowie, ul. Królewiecka 60 A, 11-700 Mrągowo w zamkniętej kopercie z dopiskiem: *OFERTA: „Audyt cyberbezpieczeństwa w ramach projektu Cyfrowa Gmina”*

*lub*

1. **przesyłać** pocztą elektroniczną na adres: e.krzywosz@mragowo.um.gov.pl Oferta złożona elektronicznie powinna zostać podpisana podpisem kwalifikowanym.

*lub*

1. **przesłać** na Elektroniczną Skrzynkę Podawczą na adres skrytki na ePuap: /ummragowo/SkrytkaESP. Oferta złożona elektronicznie powinna zostać podpisana podpisem kwalifikowanym.

**do dnia 15 czerwca 2022 roku do godz. 15.00.**

**Zamawiający zastrzega sobie prawo unieważnienia postępowania bez podania przyczyn.**

1. **KLAUZULA INFORMACYJNA**

**Zamówienie będzie realizowane zgodnie z Rozporządzeniem 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.**

Na podstawie 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 (Dz.U.UE.L.2016.119.1, dalej jako RODO), informuję, iż:

1. Administratorem Pani/Pana danych osobowych jest Gmina Miejska Mrągowo z siedzibą
w Mrągowie, 11-700 Mrągowo, ul. Królewiecka 60 A, reprezentowana przez Burmistrza Miasta Mrągowo.
2. Administrator wyznaczył Inspektora Ochrony Danych Osobowych, z którym można kontaktować się poprzez adres e-maila: iod@warmiainkaso.pl. Z Inspektorem Ochrony Danych można kontaktować się we wszystkich sprawach dotyczących danych osobowych przetwarzanych przez administratora.
3. Pani/Pana dane osobowe przetwarzane są w celu/celach:

- wypełnienia obowiązku prawnego ciążącego na Administratorze (art. 6 ust. 1 lit. c RODO),

- wykonania innych zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi (art. 6 ust. 1 lit. e RODO),

- przetwarzanie szczególnej kategorii danych związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą (art. 9 ust. 2 lit. g RODO),

- w pozostałych przypadkach Pani/Pana dane osobowe przetwarzane są wyłącznie na podstawie udzielonej zgody w zakresie i celu określonym w treści zgody (art. 6 ust. 1 lit. a RODO oraz art. 9 ust. 2 lit. a RODO).

1. Pani/Pana dane mogą być udostępniane innym organom i podmiotom na podstawie obowiązujących przepisów prawa. Pani/Pana dane osobowe mogą być również udostępniane podmiotom przetwarzającym dane w naszym imieniu (podmioty przetwarzające), np. podmioty świadczące pomoc prawną, usługi informatyczne, usługi niszczenia i archiwizacji dokumentów, jak również inni administratorzy danych osobowych przetwarzający dane we własnym imieniu, np. podmioty prowadzące działalność pocztową lub kurierską.
2. Pani/Pana dane osobowe będą przechowywane przez okres wynikający z obowiązujących przepisów prawa (Ustawa o narodowym zasobie archiwalnym i archiwach z dnia 14 lipca 1983r.,Dz.U. z 2020 r. poz. 164); w przypadku danych osobowych pozyskanych na podstawie zgody, dane te będą przechowywane przez okres wskazany w zgodzie.
3. Zgodnie z RODO przysługuje Pani/Panu prawo do:

- dostępu do swoich danych osobowych o ile odpowiedni przepis prawa nie stanowi inaczej;

- sprostowania swoich danych osobowych o ile odpowiedni przepis prawa nie stanowi inaczej;

- żądania usunięcia swoich danych osobowych o ile odpowiedni przepis prawa nie stanowi inaczej;

- żądania ograniczenia przetwarzania swoich danych osobowych o ile odpowiedni przepis prawa nie stanowi inaczej;

- wniesienia sprzeciwu wobec przetwarzania swoich danych osobowych;

- wniesienia skargi do organu nadzorczego, tj. Prezes UODO (na adres Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa);

- jeżeli przetwarzanie danych odbywa się na podstawie zgody ma Pani/Pan prawo do cofnięcia zgody na przetwarzanie danych w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

1. W sytuacji, gdy przetwarzanie danych osobowych odbywa się na podstawie zgody, podanie przez Panią/Pana danych osobowych Administratorowi ma charakter dobrowolny. Podanie przez Panią/Pana danych osobowych jest obowiązkowe, w sytuacji gdy przesłankę przetwarzania danych osobowych stanowi przepis prawa.
2. Administrator danych nie zamierza przekazywać danych osobowych do państwa trzeciego lub organizacji międzynarodowej.
3. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany i nie będą podlegały profilowaniu.