Starachowice, dn. 24.04.2023 r.

**Powiat Starachowicki**

**ul. dr. Władysława Borkowskiego 4**

**27-200 Starachowice**

Znak sprawy: IT.272.1.2023

**Zaproszenie do składania ofert**

Zapraszamy do udziału w postępowaniu prowadzonym w trybie zapytania ofertowego na:

**Przeprowadzenie diagnozy cyberbezpieczeństwa w Starostwie Powiatowym  
w Starachowicach w ramach Projektu „Cyfrowy Powiat”**

**1. Opis przedmiotu zamówienia:**

Przeprowadzenie diagnozy cyberbezpieczeństwa w ramach projektu „Cyfrowy Powiat” w Starostwie Powiatowym w Starachowicach zgodnie z zakresem wyszczególnionym w załączniku nr 3, stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego „Cyfrowy Powiat”. Zamawiający dopuszcza wykonanie diagnozy cyberbezpieczeństwa zdalnie.

CPV - 72800000-8 - Usługi audytu komputerowego i testowania komputerów

CPV - 72810000-1 - Usługi audytu komputerowego

CPV - 79212000-3 - Usługi audytu

**2. Termin wykonania zamówienia:**

Wykonawca jest zobowiązany wykonać zamówienie **w terminie 14 dni od dnia podpisania umowy.**

**3. Kryteria oceny ofert:**

Przy wyborze oferty do realizacji zamawiający będzie się kierował kryterium: **Cena – 100%.**

**4. Wymagania stawiane wykonawcom:**

Obligatoryjnie osoba, która przeprowadza diagnozę cyberbezpieczeństwa, musi posiadać uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r. poz. 1999). 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

Ponadto osoba, która przeprowadza diagnozę cyberbezpieczeństwa musi posiadać doświadczenie  
w wykonywaniu audytów wynikających z Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r.

w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych  
i wymiany informacji postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. W przeciągu 3 lat poprzedzających złożenie oferty osoba wykonująca audyt przeprowadziła minimum 1 diagnozę cyberbezpieczeństwa oraz zrealizowała co najmniej 2 audyty bezpieczeństwa w jednostkach administracji publicznej o podobnym zakresie.

Wykonawcy, którzy nie wykażą spełnienia warunków udziału w postępowaniu podlegać będą wykluczeniu z udziału w postępowaniu. Ofertę wykonawcy wykluczonego uznaje się za odrzuconą.

**5. Wymagania dotyczące oferty**

Ofertę należy sporządzić na formularzu ofertowym, będącym załącznikiem do niniejszego zapytania.

Oferta ma zawierać:

1. kompletny, wypełniony formularz ofertowy stanowiący załącznik nr 1;
2. oświadczenie o posiadaniu certyfikatów i kwalifikacji niezbędnych do przeprowadzenia audytu, stanowiące załącznik nr 2, wraz z dokumentami potwierdzającymi wymagane kwalifikacje;
3. oświadczenie o braku przesłanek do wykluczenia z postępowania, braku powiązań  
   z zamawiającym oraz spełniania warunków udziału w postępowaniu, stanowiące załącznik nr 4;

Cena ofertowa powinna zawierać w sobie wszelkie koszty niezbędne do zrealizowania zamówienia.

**6. Miejsce i termin składania ofert**

1. Ofertę należy złożyć przez platformę zakupową Open Nexus do dnia 8.05.2023 r. do godz. 11:00.
2. Oferty złożone po terminie nie będą rozpatrywane.
3. Niniejsze zapytanie ofertowe nie stanowi oferty w myśl art. 66 Kodeksu Cywilnego, nie jest aukcją ani przetargiem w rozumieniu art. 701 Kodeksu Cywilnego, jak również nie jest ogłoszeniem  
   w rozumieniu ustawy Prawo zamówień publicznych. Zamawiający zastrzega sobie prawo do unieważnienia postępowania lub do odstąpienia od podpisania umowy bez podawania przyczyn.
4. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert.
5. Zamawiający poprawia w ofercie oczywiste omyłki pisarskie, oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek, inne omyłki polegające na niezgodności oferty z opisem przedmiotu zamówienia, niepowodujące istotnych zmian w treści oferty niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.
6. Wybór oferty najkorzystniejszej zostanie opublikowany na platformie Open Nexus.

Załączniki:

1. Formularz ofertowy;
2. Oświadczenie wykonawcy o posiadaniu niezbędnych certyfikatów i kwalifikacji;
3. Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa (Załącznik nr 8 do Regulaminu Konkursu Grantowego „Cyfrowy Powiat”);
4. Oświadczenie wykonawcy o braku przesłanek do wykluczenia z postępowania, braku powiązań z zamawiającym oraz spełniania warunków udziału w postępowaniu.