Nakło nad Notecią, 21.03.2023 r.
ODI.272.4.2023

ZAPYTANIE OFERTOWE

Dotyczy: **przeprowadzenia diagnozy cyberbezpieczeństwa w Starostwie Powiatowym w Nakle nad Notecią, zakończonej raportem, obejmującym ocenę zagadnień zgodnie z zakresem wskazanym w formularzu stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowy Powiat 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 konkursu grantowego „Cyfrowy Powiat" o numerze POPC.05.01.00-00-0001/21-00**

1. Diagnoza cybezbezpieczeństwa musi zostać przeprowadzona przez osobę posiadającą 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 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.

2. Diagnoza cyberbezpieczeństwa (audyt) musi zostać przeprowadzona zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.) oraz Rozporządzeniem 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 (tj. Dz.U. 2017 poz. 2247 ze zm.) zwane dalej Rozporządzeniem KRI.

3. Diagnoza cyberbezpieczeństwa musi być przeprowadzona zgodnie z zakresem oraz formularzem stanowiącym obowiązujący na dzień wykonywania audytu załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowy Powiat, zakończonego raportem (https://www.gov.pl/web/cppc/cyfrowy-powiat);

Po przeprowadzeniu diagnozy cyberbezpieczeństwa, Wykonawca zobligowany jest do przekazania Zamawiającemu wypełnionego i podpisanego elektronicznie formularza diagnozy (przeprowadzonej przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu) w formacie pdf, a także w wersji edytowalnej .xls lub .xlsx (plik Excel) oraz dostarczenia wersji papierowej. Wykonawca poza

formularzem przekaże dokumentację składową na podstawie której został opracowany załącznik diagnozy cyberbezpieczeństwa. Zamawiający ma na myśli dokumentację szczegółową kontrolowanych punktów, systemów, czy innych elementów składowych wpływających na ocenę końcową danej kategorii, wprowadzoną do formularza diagnozy. Wykonawca przekaże również zestawienie, na podstawie którego Zamawiający punkt po punkcie będzie mógł dokonać prac naprawczych/wdrożeniowych podnoszących bezpieczeństwo systemów oraz dopracowanie procedur postępowania;

Wykonawca zobowiązany jest do współpracy i konsultacji z Zamawiającym oraz do wprowadzenia poprawek w sporządzonej przez siebie dokumentacji na każdym etapie realizacji zamówienia, aż do zaakceptowania dokumentów wystawionych przez Wykonawcę przez Grantodawcę Konkursu Cyfrowy Powiat.

4. Zamawiający nie dopuszcza wykonania audytu zdalnie w jakichkolwiek obszarach badania audytorskiego. Badanie zabezpieczeń w tym przeprowadzenie wszelkich testów, diagnozy cyberbezpieczeństwa, podatności systemów, wykonawca musi wykonać na miejscu w siedzibie Zamawiającego. Szczegółowy zakres przedmiotu zamówienia zawiera formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa stanowiący załącznik nr 8 konkursu grantowego.

5. Zamawiający wymaga, aby Wykonawca wykazał, że zrealizował co najmniej 2 audyty bezpieczeństwa w jednostkach administracji publicznej w ostatnich 3 latach przed złożeniem oferty oraz przeprowadził minimum 1 diagnozę cyberbezpieczeństwa.

6. W celu potwierdzenia wymaganych wyżej warunków wraz z ofertą należy dostarczyć (dotyczy również podwykonawców):

   a) dokumenty potwierdzające wymagane kwalifikacje do przeprowadzenia audytu,
   b) referencje potwierdzające prawidłowe wykonanie audytu.

7. **Termin i miejsce wykonania zamówienia:**
   a) termin wykonania diagnozy cyberbezpieczeństwa – **do dnia 24 kwietnia 2023 r.**
   b) miejsce wykonania przedmiotu zamówienia:

   - Starostwo Powiatowe w Nakle nad Notecią, ul. Dąbrowskiego 54,
     89-100 Nakło nad Notecią;

   W skład Starostwa Powiatowego w Nakle nad Notecią wchodzą następujące siedziby:

   - Wydział Geodezji i Gospodarki Nieruchomościami, ul. Ks. Skargi 6,
     89-100 Nakło nad Notecią;
   - Wydział Geodezji i Gospodarki Nieruchomościami filia w Szubinie, ul. Kcyńska 34 A,
     89-200 Szubin;
   - Powiatowy Zespół Do Spraw Orzekania o Niepełnosprawności, ul. Dąbrowskiego 46,
     89-100 Nakło nad Notecią;
   - Przystań Powiat Nakielski, ul. Notecka 4,
     89-100 Nakło nad Notecią.

8. **Kryterium wyboru najkorzystniejszej oferty**: najniższa cena: 100%.

9. **Sposób płatności:** Wykonawca otrzyma wynagrodzenie za wykonanie przedmiotu umowy w terminie 14 dni od daty doręczenia Zamawiającemu prawidłowo wystawionej pod względem merytorycznym i finansowym faktury, po uprzednim podpisaniu przez strony protokołu odbioru wykonanej usługi.

10. **Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia publicznego**

1) Umowa zawarta zostanie z uwzględnieniem postanowień wynikających z treści niniejszego Zapytania ofertowego oraz danych zawartych w ofercie.

2) Zamawiający przewiduje możliwość dokonania zmian zawartej z Wykonawcą umowy w stosunku do treści oferty, na której podstawie dokonano wyboru Wykonawcy w sytuacji wystąpienia okoliczności określonych w projekcie umowy.

3) Projekt umowy w sprawie zamówienia publicznego stanowi załącznik nr 1 do niniejszego Zapytania ofertowego.

11. **Zamawiający nie dopuszcza składania ofert wariantowych oraz częściowych.**

12. **Zamawiający zastrzega sobie prawo do**:

a) unieważnienia postępowania bez podania przyczyny,
b) niewybrania żadnej oferty bez podania przyczyny,
c) pozostawienia bez rozpatrzenia oferty niezgodnej z wymogami niniejszego postępowania.