Mazurskie Centrum Zdrowia Szpital Powiatowy w Węgorzewie
Publiczny Zakład Opieki Zdrowotnej
ul. 3 Maja 17, 11 – 600 Węgorzewo, tel. 87 427 32 52

Węgorzewo, 01.09.2022 r.

ZAPYTANIE OFERTOWE
na przeprowadzenie audytów cyberbezpieczeństwa

1. ZAMAWIAJĄCY:

Mazurskie Centrum Zdrowia Szpital Powiatowy w Węgorzewie Publiczny Zakład Opieki Zdrowotnej,
Adres: ul. 3 Maja 17, 11-600 Węgorzewo
Regon: 519461110

Internet: www.mazurskiecentrumzdrowia.pl
e-mail: sekretariat@szpitalwegorzewo.pl
tel. 87 427 32 52

2. OPIS PRZEDMIOTU ZAMÓWIENIA:

1) Przeprowadzenie wstępnego audytu ceberbezpieczeństwa w Mazurskim Centrum Zdrowia Szpitalu Powiatowym w Węgorzewie Publicznym Zakładzie Opieki Zdrowotnej. Przeprowadzony audyt ma wskazać jakie działania podniosą poziom bezpieczeństwa teleinformatycznego.
2) Przeprowadzenie końcowego audytu cyberbezpieczeństwa w Mazurskim Centrum Zdrowia Szpitalu Powiatowym w Węgorzewie Publicznym Zakładzie Opieki Zdrowotnej w ramach dofinansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców zakończonego raportem. Wnioski z raportu na zakończenie audytu winny uwzględniać opisy działań skutkujących podniesieniem poziomu bezpieczeństwa teleinformatycznego u Zamawiającego zgodnie z załącznikiem nr. 3. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa teleinformatycznego.

Główny kod CPV CPV- 79212000-3 usługi audytu

3. TERMIN REALIZACJI ZAMÓWIENIA:

Wykonawca zobowiązany jest wykonać:
1) Audyt wstępny- nie później niż w terminie 3 dni roboczych od zawarcia umowy.
2) Audyt końcowy- nie później do 09 grudnia 2022 r.

4. O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy spełniają warunki, dotyczące:

1. Audyt bezpieczeństwa, musi być przeprowadzony przez:
   1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 5), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych.
   2) co najmniej dwóch audytorów posiadających:
   a) Certyfikaty określone w poniższym wykazie certyfikatów uprawniających do przeprowadzenia audytu lub
   b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych lub
   c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.
2. Wykaz certyfikatów uprawniających do przeprowadzenia audytu:
   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, 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.

3. Celem audytu wstępnego jest określenie potrzeb w zakresie podniesienia poziomu cyberbezpieczeństwa.
4. Celem audytu końcowego jest w przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa.
5. Przeprowadzony audyt ma wskazać jakie działania podniosą poziomu bezpieczeństwa teleinformatycznego. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłyną na podniesienie poziomu bezpieczeństwa teleinformatycznego.

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

6. Informacje o dokumentach, jakie mają dostarczyć Wykonawcy:
W celu potwierdzenia wymaganych wyżej warunków wraz z ofertą należy dostarczyć:
1) dokumenty potwierdzające wymagane kwalifikacje do przeprowadzenia audytu,

6. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

7. Osoby upoważnione do kontaktowania się z Wykonawcami:
Osobą upoważnioną ze strony Zamawiającego do kontaktowania się z Wykonawcami jest Marek Rojek,

8. Kryterium oceny ofert:
1. Za najkorzystniejszą ofertę zostanie uznana oferta spełniająca wszystkie wymogi zawarte w Zapytaniu oraz ta, która uzyska najkorzystniejszy bilans przyznanych punktów, tj.:

$$\text{Liczba punktów danej oferty} = \frac{\text{cena najtańszej oferty brutto}}{\text{cena badanej oferty brutto}} \times 100\% \times 100$$

1) Cena oferty musi zawierać wszystkie koszty związane z prawidłową realizacją zamówienia.
2) Cenę oferty stanowi cena brutto.
3) Cena oferty musi być wyrażona w polskich złotych.
4) Zamawiający dopuszcza zmianę ceny jednostkowej brutto w sytuacji zmiany stawki podatku VAT
5) Jeżeli do niniejszego Zapytania zostaną złożone oferty o takiej samej cenie, to Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia ofert dodatkowych, w terminie 3 dni roboczych od daty otrzymania powiadomienia.

9. Termin złożenia oferty cenowej i jej otwarcia
1. Ofertę należy przesłać drogą elektroniczną przez platformę zakupową:
https://platformazakupowa.pl numer transakcji 658173 do dnia **09.09.2022 r.**, do godz. **10:00**.
2. Decydujące znaczenie dla oceny zachowania terminu ma data i godzina wpływu oferty.
3. Oferty otrzymane po terminie nie będą rozpatrywane.
4. Wykonawca może przed upływem terminu składania ofert zmienić lub wycofać swoją ofertę. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych oferty.
Otwarcie ofert nastąpi w dniu 09.09.2022 r., o godz. 10:05.

10. Zamawiający zastrzega sobie prawo unieważnienia postępowania na każdym jego etapie, bez podawania przyczyn.

11. Zamawiający zastrzega sobie prawo przedłużenia terminu składania ofert bez podawania przyczyn.

12. Informacje dodatkowe:

1. Oferta powinna być sporządzona w formie pisemnej, w języku polskim.
Ofertę należy przygotować na dokumentach załączonych do niniejszego Zapytania.
2. W załącznikach winny być wypełnione wszystkie pozycje.
3. Każdy Wykonawca może złożyć tylko jedną ofertę.
4. Oferta składana elektronicznie musi zostać podpisana elektronicznym podpisem kwalifikowanym, podpisem zaufanym lub podpisem osobistym. W procesie składania oferty za pośrednictwem platformazakupowa.pl, wykonawca powinien złożyć podpis bezpośrednio na dokumentach przesłanych za pośrednictwem platformazakupowa.pl.
5. Niniejsze Zapytanie nie podlega przepisom Ustawy z dnia 11 września 2019 r. Prawo Zamówień Publicznych.
6. Zamawiający nie ponosi żadnej odpowiedzialności ani jakichkolwiek kosztów związanych z przygotowaniem i złożeniem oferty przez Wykonawcę.
Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści niniejszego Zapytania ofertowego. Pytanie Wykonawcy powinno zostać przesłane nie później niż do **06.09.2022 r. do godz. 11:00** na adres https://platformazakupowa.pl/ numer transakcji 658173
7. Zamawiający jest zobowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż **do 07.09.2022 r. do godz. 14:00**, pod warunkiem, że zapytanie to wpłynie we wspomnianym wcześniej terminie tj. do **06.09.2022 r., godz. 11:00**.
8. Jeżeli wniosek o wyjaśnienie treści Zapytania wpłynął po upływie terminu składania wniosku, o którym mowa powyżej lub dotyczy udzielonych wcześniej wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.
9. Treść zapytań wraz z wyjaśnieniami Zamawiający, bez ujawniania źródła zapytania, umieści na platformie zakupowej niniejszego postępowania.
10. Zmiany treści Zapytania ofertowego są każdorazowo wiążące dla Wykonawców.
11. W szczególnie uzasadnionych przypadkach Zamawiający może w każdym czasie przed upływem terminu składania ofert zmodyfikować treść zapytania ofertowego. Dokonana modyfikacja zostanie zamieszczona.

13. Klauzula informacyjna z art. 13 RODO do zastosowania przez Zamawiającego w celu związanym z postępowaniem o udzielenie zamówienia publicznego

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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:

- administratorem Pani/Pana danych osobowych jest Mazurskie Centrum Zdrowia Szpital Powiatowy w Węgorzewie Publiczny Zakład Opieki Zdrowotnej

Jeśli ma Pani/Pan pytania dotyczące sposobu i zakresu przetwarzania Pani/Pana danych osobowych w zakresie działania Mazurskie Centrum Zdrowia Szpital Powiatowy w Węgorzewie Publiczny Zakład Opieki Zdrowotnej, a także przysługujących Pani/Panu uprawnień, może się Pani/Pan skontaktować się z **Inspektorem Ochrony Danych Osobowych**, z którym można się kontaktować, adres: Mazurskie Centrum Zdrowia Szpital Powiatowy w Węgorzewie Publiczny Zakład Opieki Zdrowotnej ul. 3 Maja 17, 11-600 Węgorzewo lub pod adresem e- mail: iod@szpitalwegorzewo.pl
Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego na wykonanie audytów cyberbezpieczeństwa.

- odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania
- Pani/Pana dane osobowe będą przechowywane przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;

- obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
- w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- posiada Pani/Pan:
  - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
  - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych **;
  - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO ***;
  - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- nie przysługuje Pani/Panu:
  - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
  - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
  - na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

Załączniki:
1. Załącznik nr 1 – formularz ofertowy,
2. Załącznik nr 2 – projekt umowy,
3. Załącznik nr 3 – opis działań,