

Nowe Miasto Lubawskie, dnia 31.10.2022 r.

17/2022

Zapytanie ofertowe
na przeprowadzenie audytu cyberbezpieczeństwa
w Szpitalu Powiatowym w Nowym Mieście Lubawskim sp. z o.o.

1. Zamawiający

Szpital Powiatowy w Nowym Mieście Lubawskim sp. z o.o.

ul. Mickiewicza 10

13-300 Nowe Miasto Lubawskie

Zapytanie ofertowe jest prowadzone na stronie: https://platformazakupowa.pl/pn/szpital_nml

2. Opis przedmiotu zamówienia

1. Przedmiot zamówienia stanowi przeprowadzenie audytu cyberbezpieczeństwa w Szpitalu Powiatowym w Nowym Mieście Lubawskim sp. z o.o., w skład którego wchodzi:

1) przeprowadzenie wstępnego audytu cyberbezpieczeństwa w Szpitalu Powiatowym w Nowym Mieście Lubawskim sp. z o.o., przeprowadzony audyt ma wskazać jakie działania podniosą poziom bezpieczeństwa teleinformatycznego

2) przeprowadzenie końcowego audytu cyberbezpieczeństwa w Szpitalu Powiatowym w Nowym Mieście Lubawskim sp. z o.o. w ramach dofinansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców zakończonego raportem.

2. Wnioski z raportu na zakończenie audytu winny uwzględniać opisy działań skutkujących podniesieniem poziomu bezpieczeństwa teleinformatycznego u Zamawiającego zgodnie z załącznikiem nr 1 do niniejszego Zapytania. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa teleinformatycznego.

3. Termin realizacji zamówienia

Wykonawca jest zobowiązany wykonać:

1) audyt wstępny - nie później niż w terminie 3 dni od dnia zawarcia umowy

2) audyt końcowy - nie później niż do 14 grudnia 2022 r.

4. O udzielenie niniejszego 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.

d) co najmniej dwie wystawione referencje potwierdzające wykonanie audytów cyberbezpieczeństwa.

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 wykazanie podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności wynikających z zarządzenia oraz w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa w formie ankiety. Przeprowadzony audyt wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły 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.

5. Informacje o dokumentach, jakie mają dostarczyć Wykonawcy

1. W celu potwierdzenia wymaganych wyżej warunków wraz z ofertą (formularzem ofertowym stanowiącym załącznik nr 2 do niniejszego Zapytania) należy dostarczyć:
 - 1) dokumenty potwierdzające wymagane kwalifikacje do przeprowadzenia audytu,
 - 2) referencje potwierdzające prawidłowe wykonanie 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 Dariusz Goździewski, tel. 564724166, dariuszgozdziwski@szpitalnml.pl.

8. Kryterium oceny ofert

1. Za najkorzystniejszą ofertę zostanie uznana oferta, która spełniła wszystkie wymogi zawarte w niniejszym Zapytaniu oraz uzyskała największą liczbę przyznanych punktów za kryterium ceny, obliczoną wg poniższego wzoru:

$$\text{Liczba punktów danej oferty} = \frac{\text{cena brutto najniższa w ofertach}^*}{\text{cena brutto oferty ocenianej}} \times 100\text{pkt} \times 100\%$$

* spośród wszystkich złożonych ofert niepodlegających odrzuceniu

2. Cena oferty musi zawierać wszystkie koszty związane z prawidłową realizacją zamówienia.
3. Cenę oferty stanowi cena brutto.
4. Cena oferty musi być wyrażona w polskich złotych.
5. Jeżeli do niniejszego Zapytania zostaną złożone oferty o takiej samej najniższej cenie, to Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia ofert dodatkowych, w terminie wskazanym w powiadomieniu.

9. Złożenia ofert i otwarcie ofert

1. Ofertę należy przesłać drogą elektroniczną za pośrednictwem platformy zakupowej: https://platformazakupowa.pl/pn/szpital_nml do dnia **04.11.2022 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.
5. Otwarcie ofert nastąpi w dniu **04.11.2022 r.**, o godz. **10:15**.

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.

7. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści niniejszego Zapytania ofertowego. Pytanie Wykonawcy powinno zostać przesłane za pośrednictwem platformy zakupowej https://platformazakupowa.pl/pn/szpital_nml. Treść zapytań wraz z wyjaśnieniami Zamawiający, bez ujawniania źródła zapytania, umieści na platformie zakupowej niniejszego postępowania.

8. W szczególnie uzasadnionych przypadkach Zamawiający może w każdym czasie przed upływem terminu składania ofert zmodyfikować treść zapytania ofertowego. Dokonana modyfikacja zostanie zamieszczona na platformie zakupowej. Zmiana treści Zapytania ofertowego jest wiążąca dla wszystkich Wykonawców.

13. Klauzula informacyjna z art. 13 RODO do zastosowania przez Zamawiających w celu związanym z Zapytaniem ofertowym:

1. 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 danych) (Dz. U. UE L119 z dnia 4 maja 2016 r., str. 1; zwanym dalej „RODO”) informujemy, że:

- 1) administratorem Pani/Pana danych osobowych jest Szpital Powiatowy w Nowym Mieście Lubawskim spółka z ograniczoną odpowiedzialnością.
- 2) administrator wyznaczył Inspektora Danych Osobowych, z którym można się kontaktować pod adresem e-mail: iod@szpitalnml.pl.
- 3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z przedmiotowym Zapytaniem ofertowym
- 4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja Zapytania ofertowego
- 5) Pani/Pana dane osobowe będą przechowywane, przez okres 4 lat od dnia zakończenia niniejszego Zapytania, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
- 6) obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach związanych z udziałem w Zapytaniu ofertowym
- 7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO.
- 8) posiada Pani/Pan:
 - a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących
 - b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych

- c) 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
 - d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- 9) nie przysługuje Pani/Panu:
- a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
 - b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
 - c) 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;
- 10) przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Pana danych osobowych przez administratora. Organem właściwym dla przedmiotowej skargi jest Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

Załączniki:

Załącznik nr 1 – opis działań

Załącznik nr 2 – formularz ofertowy

Załącznik nr 3 – projekt umowy

Załącznik nr 4 – ocena zgodności po wykonanym audycie

DYREKTOR
Bogumił Kurowski