



SPZOZ
W WIELUNIU

SAMODZIELNY PUBLICZNY ZAKŁAD OPIEKI ZDROWOTNEJ W WIELUNIU
ul. Szpitalna 16 · 98-300 Wieluń · e-mail: sekretariat@szpital-wielun.pl
NIP 832-17-89-610 · REGON 000310143 · Tel.: 43 840 68 00 · Fax: 43 840 68 01

Wieluń, dnia 02 września 2022 r.

ZAPYTANIE OFERTOWE

pn. „Przeprowadzenie Audytów cyberbezpieczeństwa w SPZOZ w Wieluniu”

numer postępowania: **SPZOZ-ZP/2/24/241/14/2022**

W ramach prowadzonego postępowania o udzielenie zamówienia publicznego
Zamawiający zaprasza do złożenia ofert.

1. Zamawiający:

Samodzielny Publiczny Zakład Opieki Zdrowotnej w Wieluniu
ul. Szpitalna 16
98-300 Wieluń

2. Tryb postępowania

Postępowanie prowadzone jest na podstawie Regulaminu udzielania zamówień publicznych przez Samodzielny Publiczny Zakład Opieki Zdrowotnej w Wieluniu wprowadzonego Zarządzeniem Dyrektora SPZOZ w Wieluniu nr 01/010/10/2022 z dnia 10.02.2022 r.

3. Przedmiot zamówienia

1. Przedmiotem zamówienia jest:

- a) przeprowadzenie wstępnego audytu cyberbezpieczeństwa w SPZOZ w Wieluniu. Przeprowadzony audyt ma wskazać jakie działania podniosą poziom bezpieczeństwa teleinformatycznego.
- b) przeprowadzenie końcowego audytu cyberbezpieczeństwa w SPZOZ w Wieluniu w ramach dofinansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców zakończony raportem.

2. 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.

4. Termin wykonania zamówienia

Audyt wstępny - nie później niż w terminie 2 tygodni od dnia zawarcia umowy.

Audyt końcowy - nie później niż do 10 listopada 2022 r.

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

1. Audyt bezpieczeństwa, musi być przeprowadzony przez:



Certyfikat ISO 9001:2015

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) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych lub

b) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymującą 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.

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

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. Przeprowadzony audyt ma wskazać jakie działania podniosą poziom 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. Ofertę wykonawcy wykluczonego uznaje się za odrzuconą.



6. Informacje o dokumentach, jakie mają dostarczyć Wykonawcy

1. W celu potwierdzenia wymaganych wyżej warunków wraz z ofertą należy dostarczyć:

- 1) dokumenty potwierdzające wymagane kwalifikacje do przeprowadzenia audytu,
- 2) referencje potwierdzające prawidłowe wykonanie audytu.

7. Kryterium oceny ofert

1. Jedynym kryterium oceny ofert w niniejszym postępowaniu jest **cena – 100%**.

2. Cena oferty uwzględnia wszystkie zobowiązania, musi być podana w PLN cyfrowo i słownie, z wyodrębnieniem należnego podatku VAT, jeżeli taki występuje, zgodnie z art. 3 ust 1 i 2 ustawy o informowaniu o cenach towarów i usług z dnia 9 maja 2014 roku (t. j. Dz. U. 2019 poz. 178).

3. Cena podana w ofercie winna obejmować wszystkie koszty i składniki związane z wykonaniem zamówienia oraz warunkami stawianymi przez Zamawiającego.

4. Cena za oferowany przedmiot zamówienia może być tylko jedna (nie dopuszcza się wariantowości cen) i nie ulega zmianie przez okres ważności oferty (związania ofertą).

5. Za najkorzystniejszą zostanie uznana oferta z najniższą ceną brutto. Pozostałe oferty zostaną sklasyfikowane w kolejności od najniższej do najwyższej ceny.

6. Jeżeli nie będzie można wybrać najkorzystniejszej oferty ze względu na to, że zostały złożone oferty o takiej samej cenie, Zamawiający wezwie Wykonawców, którzy złożyli te oferty do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych.

7. Wykonawcy składając oferty dodatkowe, nie mogą zaoferować cen wyższych niż zaoferowane w złożonych ofertach.

8. Zamawiający dokona obliczeń z dokładnością do dwóch miejsc po przecinku.

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

8. Termin i miejsce składania ofert:

Oferta powinna być sporządzona w formie pisemnej, w języku polskim.

Ofertę należy przygotować na dokumentach załączonych do niniejszego Zapytania.

W załącznikach winny być wypełnione wszystkie pozycje.

Każdy Wykonawca może złożyć tylko jedną ofertę.

Ofertę wraz ze wszystkimi wymaganymi oświadczeniami i dokumentami, należy złożyć za pośrednictwem Platformy zakupowej Zamawiającego (https://platformazakupowa.pl/pn/szpital_wielun) na stronie danego postępowania **w terminie do dnia 07.09.2022 r. do godz. 09:00.**

Oferty złożone po upływie terminu określonego do ich przyjmowania nie będą rozpatrywane.

Oferent może przed upływem terminu składania ofert zmienić lub wycofać ofertę.

Uwaga! Formularz oferty oraz wszystkie załączniki, w tym pełnomocnictwo, powinny być sporządzone w formie elektronicznej i podpisane **elektronicznym kwalifikowanym podpisem** lub **podpisem zaufanym** lub **podpisem osobistym**. W procesie składania oferty na platformie, **kwalifikowany podpis elektroniczny** lub **podpis zaufany** lub **podpis**

osobisty Wykonawca składa bezpośrednio na dokumencie, który następnie przesyła do systemu.

9. Sposób kontaktowania się Zamawiającego z Wykonawcami:

W sprawach związanych z prowadzonym postępowaniem Zamawiający prosi o kontakt z następującymi osobami:

- Bartłomiej Kotala (Dział Informatyki) tel.43 84 06 814 e-mail: informatycy@szpital-wielun.pl

- Katarzyna Skubiś (Dział Zamówień Publicznych) e-mail: k.skubis@szpital-wielun.pl

tel. 43 84 06 844

- Magdalena Pałyga (Dział Zamówień Publicznych) e-mail: m.palyga@szpital-wielun.pl

tel. 43 84 06 802

10. Informacje dodatkowe:

1. Informację o wyniku postępowania Zamawiający przekaze Wykonawcom, którzy odpowiedzieli na zapytanie ofertowe.
2. Zamawiający, po przekazaniu informacji o wyborze Wykonawcy, nie później jednak niż w terminie związania ofertą, zawrze z wybranym Wykonawcą umowę.
3. Jeżeli Wykonawca, którego oferta została wybrana uchyli się od zawarcia umowy, Zamawiający wybierze kolejną najkorzystniejszą spośród złożonych ofert, bez przeprowadzenia ich ponownej oceny.
4. Od decyzji Zamawiającego nie przysługują środki odwoławcze. Ponadto Zamawiający informuje, że na każdym etapie postępowania może odstąpić od podpisania umowy z Wykonawcą i unieważnić postępowanie.

Wszelkie zapytania i wyjaśnienia dotyczące przedmiotowego postępowania o udzielenie zamówienia należy składać **w terminie do 05.09.2022 r.** poprzez formularz „Wyślij wiadomość do zamawiającego” dostępny na stronie prowadzonego postępowania, tj. na platformie zakupowej (https://platformazakupowa.pl/pn/szpital_wielun) lub na adres e-mail: sekretariat@szpital-wielun.pl

.....
podpis Kierownika Zamawiającego lub osoby upoważnionej
(Na oryginale właściwy podpis: Dyrektor SPZOZ w Wieluniu Anna Freus)

Załączniki:

1. Formularz ofertowy
2. Projekt umowy
3. Opis działań
4. Ocena zgodności po wykonanym audycie
5. Klauzula informacyjna dla Wykonawców

