



## Zapytanie ofertowe

**Kod CPV: 72150000-1**

Szczegółowe warunki realizacji zamówienia oraz prawa i obowiązki Zamawiającego i wykonawcy określone są w projekcie umowy stanowiącym załącznik nr 1 do Zapytania ofertowego.

### Przedmiot zamówienia:

Usługa przeprowadzenia audytu oraz diagnozy poziomu bezpieczeństwa teleinformatycznego (cyberbezpieczeństwa) i rekomendacji dotyczących podniesienia tego poziomu jako dwu etapowego audytu bezpieczeństwa systemu informacyjnego i ochrony danych medycznych zgodnie z „Wymaganiami dotyczącymi audytu bezpieczeństwa”, stanowiącymi załącznik nr 2 do Umowy o finansowanie ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców, będącej załącznikiem Nr 2 do Zarządzenia Nr 68/2022/BBIICD Prezesa NFZ z dnia 20 maja 2022 r. „z wymaganiami ustawy z dnia 13 sierpnia 2018 roku o Krajowym Systemie Cyberbezpieczeństwa, Krajowych Ram Interoperacyjności zgodnie z wymaganiami norm PN ISO IEC 27001, PN ISO IEC 22301 wraz z wykorzystaniem standardów WGITA poprzez dwukrotne tożsame zadaniowo badanie:

- a) spełniania wymogów dokumentacyjnych obowiązujących u Zamawiającego jako regulacji wewnętrznych dokumentacji normatywnej i operacyjnej dotyczących usługi kluczowej bezpieczeństwa informacji - dokumentacja SZBI/KRI/BCM, ochrony danych osobowych dokumentacja RODO i ODO,
- b) określenia poziomu i dojrzałości bezpieczeństwa systemu informatycznego Zamawiającego w tym przeprowadzenia testów penetracyjnych
- c) określenia poziomu i dojrzałości bezpieczeństwa systemu informatycznego Zamawiającego w tym przeprowadzenia testów penetracyjnych

w zakresie:

- skuteczności działania infrastruktury,
- procesów zarządzania bezpieczeństwem informacji,
- monitorowania i reagowania na incydenty bezpieczeństwa,
- zarządzania ciągłością działania,
- utrzymania systemów informacyjnych,
- zarządzania bezpieczeństwem i ciągłością działania łańcucha usług





Szczegółowe warunki i wymagania dotyczące realizacji zamówienia zostały określone w opisie przedmiotu zamówienia stanowiącego załącznik nr 1 do niniejszego zapytania ofertowego.

**Wymagany termin wykonania zamówienia:** 17.10.2022- 20.12.2022r.

Zadanie 1 jako Audyt wstępny (diagnostyczny) 1-sze badanie i raport do 31.10.2022r.

Zadanie 2 jako Audyt końcowy raport końcowy z oceną do 20.12.2022r.

**Warunki udziału w postępowaniu oraz sposób ich weryfikacji.**

- 1) Wykonawcy ubiegający się o realizację zamówienia powinni posiadać niezbędną wiedzę i doświadczenie oraz dysponować odpowiednimi zasobami osobowymi umożliwiającymi wykonanie przedmiotu zamówienia o udział w zamówieniu mogą ubiegać się Wykonawcy, którzy spełniają następujące warunki:
  - a) w okresie od 01.01.2018 r. wykonali (tj. świadczyli, zrealizowali, zakończyli) co najmniej 5 usług w obejmujących swoim zakresem:
    - audyt bezpieczeństwa informacji zgodnie z wymaganiami KRI (audyt KRI/SZBI),
    - audyt bezpieczeństwa systemów informatycznych, w tym testów penetracyjnych,
  - b) w okresie od 01.01.2018 r. wykonali (tj. świadczyli, zrealizowali, zakończyli) co najmniej 3 usługi w podmiotach będących operatorem usługi kluczowej (UKSC),
  - c) dysponują zespołem audytowym składającym się przynajmniej z 3 osób zatrudnionych na podstawie umowy o pracę, które będą realizowały audyt u Zamawiającego, posiadających 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 w tym:
    - co najmniej jedna osoba z zespołu musi posiadać certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji wg normy ISO 27001 wskazanymi jako uprawnione do audytowania w Rozporządzeniu Ministra Cyfryzacji w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu, ukończyła studia podyplomowe bezpieczeństwa informacji lub równoważny kurs kwalifikacyjny oraz brała udział w charakterze audytora wiodącego w co najmniej 9 audytach KRI,
    - co najmniej jedna osoba z zespołu musi posiadać certyfikat audytora wiodącego lub wewnętrznego wg normy ISO 27701, ukończyła studia podyplomowe ochrony danych osobowych lub równoważny kurs kwalifikacyjny oraz brała udział w charakterze audytora wewnętrznego lub wiodącego w co najmniej 5 audytach KRI/SZBI,
    - co najmniej jedna osoba z zespołu jest specjalistą ds. bezpieczeństwa IT, który brał udział w charakterze pentestera w co najmniej 5 audytach bezpieczeństwa IT z zastosowaniem testów penetracyjnych oraz posiada przynajmniej jeden z





następujących certyfikatów:

1. Certified Ethical Hacker (CEH),
  2. Certified IT Security Specialist Training (CSST)
  3. Certified Penetration Testing Engineer (CPTE),
  4. GIAC Exploit Researcher and Advanced Penetration Tester (GXPN),
  5. Offensive Security Certified Professional (OSCP),
  6. Offensive Security Certified Expert (OSCE),
  7. Certified Information Security Manager (CISM),
  8. Certified in Risk and Information Systems Control (CRISC),
  9. Certified in the Governance of Enterprise IT (CGEIT),
  10. Certified Information Systems Security Professional (CISSP),
  11. Certified IT Security Specialist Training(CISPT)
  12. Certified Information Technical Security Specialist jako(CITSS),
  13. Systems Security Certified Practitioner (SSCP)
  14. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.
- 2) W celu potwierdzenia spełniania warunku udziału w postępowaniu Wykonawcy muszą złożyć wraz z ofertą Wykaz usług, którego wzór stanowi załącznik nr 3 do zapytania ofertowego oraz przesłać dla każdej z usług wskazanych w Wykazie skany referencji i/lub protokołów odbioru potwierdzających wykonanie danej usługi.
- 3) W celu potwierdzenia spełniania warunku udziału w postępowaniu Wykonawcy muszą złożyć wraz z ofertą Wykaz osób, którego wzór stanowi załącznik nr 4 do zapytania ofertowego oraz przesłać dla każdej z osób wskazanych w wykazie skany certyfikatów.
- 4) W postępowaniu nie mogą brać udziału Wykonawcy, z którymi Zamawiający ma (w trakcie postępowania) podpisane umowy powierzenia danych osobowych lub podmioty w jakikolwiek sposób z takimi firmami powiązane.
- 5) Zamawiający nie dopuszcza wykonywanie audytu przez podwykonawców.

W związku z koniecznością podpisania z Wykonawcą umowy powierzenia danych, przy ocenie ofert, brane będą pod uwagę wyłącznie podmioty spełniające wymogi art. 28 ust. 1 RODO.

Ocena potencjalnego podmiotu przetwarzającego odbędzie się na podstawie wypełnionej i przesłanej przez oferentów wraz z ofertą wypełnionej ankiety „Ankieta dla podmiotu przetwarzającego dane osobowe” stanowiącej załącznik nr 5 do niniejszego zapytania ofertowego.

Podmiot wyłoniony w wyniku zapytania ofertowego zobowiązany jest do podpisania z Zamawiającym umowy powierzenia danych w treści stanowiącej załącznik nr 6 do niniejszego zapytania ofertowego - treść umowy powierzenia nie





podlega negocjacom.

## Opis kryteriów wyboru oferty najkorzystniejszej – Cena 100%.

Jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam poziom cenowy, zamawiający wzywa wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez zamawiającego ofert dodatkowych. Cena wskazana w ofercie dodatkowej nie może być wyższa niż w pierwotnej ofercie.

W przypadku gdy Wykonawca, którego oferta została wybrana, uchyla się od zawarcia umowy lub nie dopełni jakichkolwiek innych formalności związanych z niniejszym postępowaniem Zamawiający zastrzega sobie prawo do wyboru najkorzystniejszej oferty spośród pozostałych ofert spełniających wymogi określone w zapytaniu ofertowym, bez przeprowadzania ich ponownego badania i oceny.

## Wymagane dokumenty przy składaniu oferty.

Wykonawca składając ofertę na realizację zamówienia zobowiązany jest złożyć:

- a) formularz ofertowy - uzupełniony i podpisany przez osobę uprawnioną do reprezentowania Wykonawcy - wzór stanowi załącznik nr 2 do zapytania ofertowego. Oferta Wykonawcy powinna zawierać cenę netto i brutto. Cena oferty brutto jest ceną ostateczną określającą maksymalne wynagrodzenie Wykonawcy z tytułu realizacji przedmiotu zamówienia. Należy ją skalkulować tak, aby obejmowała wszystkie koszty, nakłady i wydatki, jakie Zamawiający poniesie na realizację przez Wykonawcę niniejszego zamówienia, z uwzględnieniem podatku od towarów i usług oraz innych należności publiczno-prawnych i ewentualnych upustów. Zamawiający nie ponosi żadnej odpowiedzialności ani jakichkolwiek kosztów związanych z przygotowaniem oferty przez Wykonawcę, a w szczególności związanych z przystąpieniem do procesu ofertowego, przygotowaniem i złożeniem oferty, negocjacji, przygotowaniem do zawarcia umowy.
- b) wykaz usług zawierający wartość, przedmiot, daty wykonania oraz dane podmiotów, na rzecz których usługi te zostały wykonane - uzupełniony i podpisany przez osobę uprawnioną do reprezentowania Wykonawcy - wzór stanowi załącznik nr 3 do zapytania ofertowego,
- c) wykaz osób, które będą uczestniczyć w wykonywaniu zamówienia - uzupełniony i podpisany przez osobę uprawnioną do reprezentowania Wykonawcy - wzór stanowi załącznik nr 4 do zapytania ofertowego,
- d) ankieta dla podmiotu przetwarzającego dane osobowe stanowiąca załącznik nr 5 do zapytania ofertowego,
- e) skany dokumentów, o których mowa w niniejszym zapytaniu ofertowym.

Oferty wykonawców niespełniające warunków wymienionych w niniejszym zapytaniu ofert



owym nie będą rozpatrywane.

W toku dokonywania oceny złożonych ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert, w tym załączonych do nich dokumentów.

**Miejsce i termin składania oferty cenowej:**

Termin składania ofert: 14.10.2022 godz. 14:00

Oferty wysyłane drogą elektroniczną należy wysłać na adres e-mail: [biuropodawcze@zsm.com.pl](mailto:biuropodawcze@zsm.com.pl)

Oferty w formie papierowej należy składać w biurze podawczym Pawilon VI budynek administracyjny 41-500 Chorzów, ul. Strzelców Bytomskich 11 - liczy się termin wpływu oferty do biura podawczego.

Zamawiający ma prawo odrzucić oferty wpływające po wyznaczonym terminie.

**Wskazanie osób upoważnionych przez Zamawiającego do kontaktu z Wykonawcami:**

Sebastian Rusinek e-mail: [srusinek@zsm.com.pl](mailto:srusinek@zsm.com.pl)

Artur Thill e-mail: [athill@zsm.com.pl](mailto:athill@zsm.com.pl)

W sprawie audytu bezpieczeństwa systemu informatycznego i testów penetracyjnych ewentualne pytania proszę kierować pod adres e-mail: [srusinek@zsm.com.pl](mailto:srusinek@zsm.com.pl)

Wykonawca jest zobowiązany do wskazania w ofercie terminu związania ofertą, nie krótszego niż 30 dni kalendarzowych od upływu terminu składania ofert.

Zamawiający zastrzega sobie prawo do wystąpienia do Wykonawcy o wyrażenie zgody na przedłużenie terminu związania ofertą.

Zamawiający informuje, iż do najkorzystniejszej oferty niniejszego postępowania nie mają zastosowania przepisy ustawy Prawo zamówień publicznych z uwagi na wartość przedmiotu zamówienia nie przekraczającą kwoty 130 000 zł netto.

W uzasadnionych przypadkach Zamawiający może w każdym czasie, przed upływem terminu składania ofert, zmodyfikować treść dokumentów zawierających istotne warunki zamówienia. Dokonane w ten sposób uzupełnienie umieszczone zostanie niezwłocznie na stronie [www.zamawiajacego.pl](http://www.zamawiajacego.pl).

Zamawiający zastrzega sobie prawo do odrzucenia ofert o rażąco niskiej cenie lub nieadekwatnej (do liczby komórek organizacyjnych Zamawiającego) liczbie godzin działań



# Zespół Szpitali Miejskich w Chorzowie

audytowych.

Zamawiający zastrzega sobie w każdym czasie prawo do zamknięcia postępowania oraz prawo odwołania lub unieważnienia postępowania na każdym etapie bez podania przyczyn i bez ponoszenia jakichkolwiek skutków prawnych i finansowych.

Wykonawca składający ofertę musi być czynnym podatnikiem VAT, a jego rachunek bankowy musi znajdować się w Wykazie podmiotów zarejestrowanych jako podatnicy VAT - <https://www.podatki.gov.pl/wykaz-podatnikow-vat-wyszukiwarka/>

Podmiot wyłoniony w wyniku zapytania ofertowego zobowiązany jest do podpisania z Zamawiającym umowy w treści stanowiącej załącznik nr 7 do niniejszego zapytania ofertowego - treść umowy nie podlega negocjacji.

data i podpis

DYREKTOR  
SP ZOZ Zespół Szpitali Miejskich

dr n. ekg. Jerzy Szafranowicz

P.O.  
Dyrektora operacyjnego  
SP ZOZ Zespół Szpitali Miejskich

Iwona Filip



•• SP ZOZ Zespół Szpitali Miejskich  
w Chorzowie  
ul. Strzelców Bytomskich 11  
41-500 Chorzów

•• tel.: (32) 349 93 25  
fax: (32) 241 39 52

•• zsm@zsm.com.pl  
www.zsm.com.pl

•• NIP: 6271923530  
REGON: 271503410  
KRS: 0000011939



## Klauzula informacyjna dotycząca przetwarzania danych osobowych

---

1. Administratorem danych osobowych jest Samodzielny Publiczny Zakład Opieki Zdrowotnej Zespół Szpitali Miejskich, Strzelców Bytomskich 11, 41-500 Chorzów, NIP: 6271923530, REGON: 271503410, KRS : 0000011939
2. Kontakt z Inspektorem Ochrony Danych Administratora możliwy jest pod adresem e-mail – [iod@zsm.com.pl](mailto:iod@zsm.com.pl)
3. Podane dane osobowe przetwarzane są w celu:
  - a) podjęcia działań przed zawarciem Umowy na żądanie osoby, której dane dotyczą, lub realizacji umowy, na podstawie art. 6 ust. 1 lit. b) RODO;
  - b) w przypadku danych osobowych reprezentantów podmiotów instytucjonalnych – w celu podjęcia działań przed zawarciem Umowy z podmiotem, którego dana osoba reprezentuje, na podstawie art. 6 ust. 1 lit. f) RODO;
  - c) wypełnienia prawnych obowiązków ciążących na Administratorze, na podstawie art. 6 ust. 1 lit. c) RODO;
  - d) dochodzenia roszczeń wynikających z zawartych umów oraz obrony przed roszczeniami, na podstawie art. 6 ust. 1 lit. f) RODO.
4. Podanie danych osobowych jest dobrowolne, jednak niezbędne do podjęcia działań przed realizacją umowy lub realizacji umowy.
5. Podane dane osobowe, w zależności od celu ich przetwarzania będą przetwarzane przez Administratora:
  - a) przez okres niezbędny do realizacji działań przed zawarciem umowy;
  - b) przez czas wykonywania obowiązków prawnych oraz czas, w którym przepisy prawa nakazują ich przetwarzanie;
  - c) przez czas po którym przedawnią się roszczenia wynikające z umowy; okres przetwarzania może zostać każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych osobowych będzie niezbędne dla ustalenia lub dochodzenia ewentualnych roszczeń lub obrony przed takimi roszczeniami przez Administratora.
6. Odbiorcami podanych danych osobowych mogą być podmioty uprawnione do tego na podstawie przepisów prawa oraz inne podmioty z którymi administrator zawarł umowy powierzenia przetwarzania danych osobowych.
7. Podane dane osobowe nie będą przekazywane do państw trzecich.
8. Osoba, której dane dotyczą posiada prawo dostępu do swoich danych, ich sprostowania, zaktualizowania i prawo do ograniczenia przetwarzania danych, a w zakresie, w którym przepisy prawa nie stanowią inaczej również prawo do ich usunięcia, wniesienia sprzeciwu wobec przetwarzania oraz prawo do przenoszenia danych.
9. Osoba, której dane dotyczą posiada prawo wniesienia skargi do organu nadzorczego gdy uzna, iż przetwarzanie jego danych osobowych narusza przepisy RODO.
10. W oparciu o dane osobowe Administrator nie będzie podejmował zautomatyzowanych decyzji, w tym decyzji będących wynikiem profilowania.

