

# WOJEWÓDZKI SZPITAL OBSERWACYJNO ZAKAŻNY IM. TADEUSZA BROWICZA

ul. Św. Floriana 12 85-030 Bydgoszcz  
centrala tel. 52 325-56-00 fax.52 32-55-664  
sekretariat@wsoz.pl

---

Bydgoszcz 16.09.2022r.

**Nr postępowania 12/2022**

## **I. Zamawiający**

Nazwa: Wojewódzki Szpital Obserwacyjno – Zakaźny im. Tadeusza Browicza

Adres: 85-030 Bydgoszcz, ul. Św. Floriana 12

KRS\_0000063531 ; NIP\_554-22-12-988; REGON\_000979188

Telefon: 52\_325-56-00; Faks: 52\_325-56-50 ; E-mail: sekretariat@wsoz.pl

Strona internetowa: www.wsoz.pl

Wojewódzki Szpital Obserwacyjno – Zakaźny im. Tadeusza Browicza w Bydgoszczy zaprasza do składania ofert na wykonanie usługi przeprowadzenia audytu oraz diagnozy poziomu bezpieczeństwa teleinformatycznego (cyberbezpieczeństwa) i rekomendacji dotyczących podniesienia tego poziomu. Przedmiot zamówienia stanowi jedną całość bez podziału na części/zadania.

*Źródło finansowania: Zadanie realizowane jest ze środków Ministerstwa zdrowia – środki pochodzące z Funduszu Przeciwdziałania COVID – 19 podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców.*

Na przedmiot zamówienia składa się:

- a. Audyt początkowy mający na celu zapoznanie się ze stanem początkowym dotyczącym poziomu bezpieczeństwa teleinformatycznego, uwzględniający ocenę ankietową
- b. Opracowanie ramowej analizy stanu aktualnego dotyczącego poziomu bezpieczeństwa teleinformatycznego z uwzględnieniem wyników audytu początkowego wraz ze wskazaniem elementów do usprawnienia.
- c. Audyt końcowy wykonany po realizacji wszystkich zakupów w projekcie pt. „Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców”. Audyt poziomu bezpieczeństwa teleinformatycznego powinien uwzględniać elementy wdrożone w ramach realizacji aspektów wskazanych przez Zamawiającego.
- d. Opracowanie wyników stanu pierwotnego i stanu po realizacji projektu wraz z uwzględnieniem rekomendacji dotyczącej zasadności i kompletności realizacji projektu „Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców”.

## **II. Podstawy wykluczenia / Warunki udziału w postępowaniu**

1. Zgodnie z art. 2 ust. 1 pkt.1 ustawy z dnia 11 września 2019 roku Prawo Zamówień Publicznych ( Dz. U z 2021r. Poz. 1129) – do niniejszego postępowania nie stosuje się przepisów ustawy PZP, gdyż szacunkowa wartość zamówienia jest mniejsza od kwoty 130 000 złotych.
2. Do czynności podejmowanych przez Zamawiającego i Wykonawców w postępowaniu o udzielenie zamówienia mają zastosowanie postanowienia niniejszego „Zapytania ofertowego” a w sprawach nieuregulowanych przepisy ustawy z

dnia 23 kwietnia 1964 r. - Kodeks Cywilny (Dz. U. Z 2020r poz. 1740).

3. Na podstawie art. 7 ust. 1, w związku z art. 7 ust. 9 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, Zamawiający wykluczy z postępowania:

1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt. 3 ustawy.

2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 2018 r. o o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. Z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy.

3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994r. O rachunkowości (Dz. U. 2021 r. poz. 2017, 2105 i 2106), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt. 3 ustawy.

Wykluczenie następuje na okres trwania okoliczności wskazanych w pkt 1-3 powyżej.

#### Warunki udziału w zapytaniu ofertowym:

Audyt bezpieczeństwa, o którym mowa w niniejszego zarządzenia może 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 uprawiających 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.

Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

1. Certified Internal Auditor (CIA);

1) Certified Information System Auditor (CISA);

2) 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;

3) 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;

4) Certified Information Security Manager (CISM);

5) Certified in Risk and Information Systems Control (CRISC);

6) Certified in the Governance of Enterprise IT (CGEIT);

7) Certified Information Systems Security Professional (CISSP);

8) Systems Security Certified Practitioner (SSCP);

9) Certified Reliability Professional;

10) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

### **III. Termin i miejsce wykonania zamówienia / terminy płatności:**

I Etap – audyt początkowy – 21 dni od podpisania umowy

II Etap – audyt końcowy - 14 dni po wdrożeniu zaleceń – nie później niż do 15.12.2022

- Zapłata należności następować będzie przelewem na rachunek Wykonawcy na podstawie wystawienia i doręczenia prawidłowo wystawionej faktury VAT w terminie 30 dni licząc od dnia zrealizowania całości przedmiotowej usługi.

### **IV. Informacje o oświadczeniach i dokumentach jakie mają dostarczyć Wykonawcy:**

1) Formularz oferty – wedle załącznika nr 1 do zapytania ofertowego.

2) oświadczenie stanowiące załącznik nr 2 do zapytania ofertowego

3) oświadczenie stanowiące załącznik nr 3 do zapytania ofertowego

4) Ponadto do oferty należy dołączyć:

a) odpowiedni dokument rejestrowy (KRS, CEIDG), wystawiony nie wcześniej niż 1 miesiąc przed upływem terminu składania ofert;

b) pełnomocnictwo (w oryginale lub kopii poświadczony notarialnie) do reprezentowania Wykonawcy w postępowaniu jeżeli nie wynika ono z odpisu z właściwego rejestru lub aktualnego zaświadczenia o wpisie do ewidencji działalności gospodarczej – *jeżeli dotyczy*;

c) dokumenty potwierdzające warunki udziału w zapytaniu ofertowym wedle wykazu dokumentów wskazanych w rozdziale II niniejszego zapytania ofertowego.

Niniejsze wyżej opisywane dokumenty i oświadczenia należy złożyć wraz z ofertą, niezłożenie wymaganych dokumentów spowoduje odrzucenie oferty. Oferta musi być podpisana kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osoby upoważnione do składania oświadczeń woli w imieniu Wykonawcy.

Oferta wraz ze wszystkimi załącznikami – pod rygorem jej odrzucenia – musi być sporządzona w języku polskim i podpisana przez osobę(y) upoważnioną(e) do reprezentowania wykonawcy wobec osób trzecich.

Wszystkie dokumenty dołączane do oferty, a sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski.

Podana w ofercie cena musi być wyrażona w PLN. Cena ofertowa, jak również ceny jednostkowe muszą uwzględniać wszystkie wymagania niniejszego ogłoszenia oraz obejmować wszelkie koszty, jakie poniesie wykonawca z tytułu należytej oraz zgodnej z obowiązującymi przepisami realizacji z przedmiotu zamówienia.

Cena ofertowa brutto zaproponowana przez wykonawcę w Formularzu ofertowym, (załącznik nr 1 do zapytania ofertowego) musi obejmować wszystkie części składowe oraz wszelkie podatki i zobowiązania wynikające z przedmiotu zamówienia. Wykonawca oświadcza, że cena będzie ostateczna.

Złożenie oferty jest równoznaczne z akceptacją bez zastrzeżeń warunków określonych w niniejszym zapytaniu.

### **V. Miejsce i termin składania i otwarcia ofert:**

Ofertę należy złożyć do 23.09.2022 r., do godz. 9:00:

w wersji elektronicznej na adres e-mail: [a.renk@wsoz.pl](mailto:a.renk@wsoz.pl)

Otwarcie ofert nastąpi 23.09.2022r. o godz. 9:10

## **VI. Kryteria wyboru oferty:**

Zamawiający przy wyborze oferty będzie się kierował następującymi kryteriami oceny ofert:

1/ Cena oferty

Ranga 100 %

Przy ocenie kryterium „Cena oferty” zostanie wykorzystany wzór :

$LPC = [ C\_min / C\_bad ] \times 100$ , gdzie:

LPC - liczba punktów całkowita oferty,

C\_min – cena brutto najtańszej oferty spośród ofert złożonych ,

C\_bad - cena brutto oferty badanej.

Najkorzystniejszą jest oferta, której L jest największe.

Oferowana przez wykonawcę cena oferty to cena brutto oferty, obejmująca wszystkie rabaty i upusty i traktowana jako ostateczna do zapłaty przez Zamawiającego, określona do dwóch miejsc po przecinku. Uzyskana ocena zostanie zaokrąglone z dokładnością do dwóch miejsc po przecinku.

Max ilość punktów - 100

## **VII. Informacje dotyczące wyboru najkorzystniejszej oferty:**

1. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający zawiadomi wszystkich wykonawców, którzy złożyli oferty, o wyborze najkorzystniejszej oferty, podając nazwę firmy lub imię i nazwisko, adres wykonawcy oraz cenę, którego ofertę wybrano oraz zamieści informacje, o których mowa wyżej na swojej stronie internetowej.
2. Jeśli wykonawca, którego oferta została wybrana wycofa się z postępowania lub odmawia podpisania umowy, Zamawiający zastrzega sobie prawo wyboru oferty najkorzystniejszej spośród pozostałych ofert bez przeprowadzania ich ponownego badania i oceny.

## **VIII. Pozostałe informacje:**

Zamawiający zastrzega sobie prawo do unieważnienia zapytania w dowolnym momencie przed podpisaniem umowy bez podania przyczyny. Zamawiający zawrze umowę z Wykonawcą wedle wzoru umowy stanowiący załącznik nr 4

Celem audytu jest wykazanie przez świadczeniodawcę podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności, zgodnie z niniejszym zarządzeniem Nr 68/2020/BBIIICD Prezesa Narodowego Funduszu Zdrowia z dnia 20 maja 2022r.

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.

Audyt i raport musi zawierać analizę poniższych obszarów:

Nazwa obszaru	Opis działań skutkujących podniesieniu poziomu bezpieczeństwa teleinformatycznego u świadczeniodawców
Skuteczność działania infrastruktury	-Urządzenia i konfiguracja w zakresie ochrony poczty -Urządzenia i konfiguracja w zakresie ochrony sieci -Urządzenia i konfiguracja w zakresie systemów serwerowych -Urządzenia i konfiguracja w zakresie stacji roboczych -Urządzenia i konfiguracja w zakresie systemów bezpieczeństwa
Procesy zarządzania bezpieczeństwem informacji	-Nośniki wymienne - udokumentowany sposób postępowania -Zarządzanie tożsamością / dostęp do systemów w zakresie: -- Przydzielanie dostępu -- Odbieranie dostępu -Pomieszczenie w dyspozycji struktur zespołu odpowiedzialnego za cyberbezpieczeństwo w przypadku podmiotów, które otrzymały decyzję uznającą taki podmiot za operatora usługi kluczowej, o którym mowa w art. 5 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa
Monitorowanie i reagowanie na incydenty bezpieczeństwa	-Procedury zarządzania incydentami -Raportowanie poziomów pokrycia scenariuszami znanych incydentów -Dokumentacja dotycząca przekazywania informacji do właściwego zespołu CSIRT poziomu krajowego/ sektorowego zespołu cyberbezpieczeństwa -Monitorowanie i wykrycie incydentów bezpieczeństwa -Identyfikacja i dokumentowanie przyczyn wystąpienia incydentów
Zarządzanie ciągłością działania	-Konfiguracja oraz polityki systemów do wykonywania kopii bezpieczeństwa -Raport z przeglądów i testów odtwarzania kopii bezpieczeństwa -Procedury wykonywania i przechowywania kopii zapasowych -Strategia i polityka ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP) -Procedury utrzymaniowe
Utrzymanie systemów informacyjnych	-Harmonogramy skanowania podatności -Aktualny status realizacji postępowania z podatnościami -Procedury związane ze z identyfikowaniem (wykryciem) podatności -Współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami
Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług	-Polityka bezpieczeństwa w relacjach z dostawcami -Standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa -Dostęp zdalny -Metody uwierzytelnienia

#### **IX. Osobami upoważnionymi do udzielania informacji związanych z postępowaniem są:**

p. Adam Renk – Inspektor ds. zamówień publicznych tel. 52/32 55 682, fax. 52/32 55 664, email: [a.renk@wsoz.pl](mailto:a.renk@wsoz.pl)

p. Jakub Kapuściński – kierownik sekcji ds. informatyki tel. 52/32 55 904, email: [j.kapuscinski@wsoz.pl](mailto:j.kapuscinski@wsoz.pl)

#### **X. Załączniki:**

- załącznik nr 1 – formularz ofertowy
- załącznik nr 2 – oświadczenie
- załącznik nr 3 – oświadczenie
- załącznik nr 4 – wzór umowy

KLAUZULA INFORMACYJNA – dotyczy osób fizycznych

KLAUZULA INFORMACYJNA

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 :

- 1) administratorem Pani/Pana danych osobowych jest Wojewódzki Szpital Obserwacyjno - Zakaźny im. T. Browicza w Bydgoszczy, ul. Św. Floriana 12, 85-030 Bydgoszcz ;
- 2) Inspektorem Ochrony Danych Osobowych wyznaczonym przez Administratora jest Marta Zielińska - Adamczyk, z którym można się kontaktować w każdej sprawie dotyczącej przetwarzania danych osobowych: e-mail: [iodo@wsoz.pl](mailto:iodo@wsoz.pl) ;
- 3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego ;
- 4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 ust. 1 oraz art. 74 ust. 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych), dalej „ustawa Pzp” ;
- 5) Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 ustawy Pzp, 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 ;
- 6) 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 ;
- 7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie 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 .