Do Regulaminu Udzielenia Zamówień Publicznych w SPZOZ w Łukowie
(dot. Rozdz. III litD pkt2.1a)

# ZAPYTANIE OFERTOWE

**o zamówienie publiczne prowadzone na podstawie art. 2 pkt 2 ustawy Prawo zamówień publicznych**

**Szkolenia kadry kierowniczej i personelu z zakresu cyberbezpieczeństwa**

***(przedmiot zamówienia)***

Zakup jest realizowany ze środków planu rozwojowego Przedsięwzięcia pn. „Wdrożenie e-usług w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Łukowie", realizowanego w ramach Krajowego Planu Odbudowy i Zwiększania Odporności: Komponent D „Efektywność, dostępność i jakość systemu ochrony zdrowia", Inwestycja D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia" - nr wniosku KPOD.07.03-IP.10-0209/25.

***ZO/SI/1/2026***

***(nr nadany postępowaniu)***

Z-CA DYREKTORA
ds. Inwestycyjno-Technicznych
.....Dariusz Orzeł.....

**ZATWIERDZAM**

(Dyrektor lub właściwy zastępca Dyrektora)

materiały bezpłatne

***Łuków, 04.03.2026***

*(miejscowość/data)*

## 1. ZAMAWIAJĄCY

**Samodzielny Publiczny Zakład Opieki Zdrowotnej w Łukowie**
Adres: ul. Rogalińskiego 3, 21-400 Łuków
Telefon: (25) 7982603 faks: (25) 7982603; e-mail: spzoz@spzoz.lukow.pl
Godziny urzędowania od 07:30 do 15:00.
Konto bankowe: .....
NIP: 825-17-11-719; Regon: 000306472

## 2. PRZEDMIOT ZAMÓWIENIA

1. Przeprowadzenie szkolenia kadry kierowniczej zamawiającego. Zadanie zostanie zrealizowane w siedzibie zamawiającego w ciągu dwóch dni roboczego z podziałem na trzy grupy szkoleniowe do 50 osób w każdej z grup.
2. Przeprowadzenie szkolenia pracowników administracji oraz pracowników medycznych zamawiającego. Zadanie zostanie zrealizowane w siedzibie zamawiającego w ciągu dwóch dnie roboczego z podziałem na trzy grupy szkoleniowe liczące do 50 osób w każdej z grup.
3. Dodatkowo dla wszystkich pracowników Zamawiającego zostanie udostępnione szkolenie z wykorzystaniem platformy szkoleniowej Wykonawcy na okres do 15.05.2026 dni.

Szczegółowy zakres przedmiotu zamówienia przedstawia **Załącznik nr 3 do ZO**.

## 3. TERMIN RELIZACJI PRZEDMIOTU ZAMÓWIENIA

Termin realizacji umowy **60 dni** od daty zawarcia umowy, nie później niż do 15.05.2026.

### 1. WYMAGANE DOKUMENTY (wybrać stosownie do przedmiotu zamówienia)

1.1. Aktualny odpis z właściwego rejestru albo aktualne zaświadczenie o wpisie do ewidencji działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub zgłoszenia do ewidencji działalności gospodarczej. *Powyższy dokument musi być wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.*

## 4. WARUNKI UDZIAŁU W POSTĘPOWANIU

O zamówienie mogą ubiegać się wykonawcy, którzy:

1. są zdolni do wykonania przedmiotu zamówienia i spełniają warunki w zakresie:
   a. posiadania kompetencji/uprawnień do prowadzenia działalności zawodowej, o ile wynika to z odrębnych przepisów – złożą w tym zakresie oświadczenie na formularzu ofertowym;
   b. sytuacji finansowej umożliwiającej realizację przedmiotu zamówienia – złożą w tym zakresie oświadczenie na formularzu ofertowym;
   c. posiadania potencjału technicznego i osobowego niezbędnego do wykonania przedmiotu zamówienia – złożą w tym zakresie oświadczenie na formularzu ofertowym;

## 5. OPIS SPOSOBU PRZYGOTOWANIA OFERT

5.1 Wykonawca może złożyć tylko jedną ofertę.

**5.2** Oferta musi być sporządzona z zachowaniem formy elektronicznej pod rygorem nieważności.

5.3 Oferta musi być podpisana elektronicznie przez uprawnionego przedstawiciela Wykonawcy.

**5.4** Oferta musi być sporządzona w języku polskim.

5.5 **Ofertę należy wypełnić elektronicznie, zapisać do formatu pdf, podpisać elektronicznie za pomocą podpisu zaufanego lub podpisu kwalifikowanego, spakować zip/7z z użyciem hasła i przesłać pocztą elektroniczną lub systemem e-doręczeń, tytuł wiadomości opisać: „Oferta na Szkolenia kadry kierowniczej i personelu z zakresu cyberbezpieczeństwa". Hasło do oferty, dostarczyć w odrębnej wiadomości po czasie składania ofert, do godziny 11:00 w dniu otwarcia ofert.**

## 6. MIEJSCE I TERMIN SKŁADANIA OFERT

6.1 Oferty winny być złożone za pomocą poczty elektronicznej lub systemem e-doręczeń na adres spzoz@spzoz.lukow.pl lub **AE:PL-97801-70047-GUBWJ-29** w terminie do **10.03.2026 r. do godziny 10:00**

6.2 Oferta otrzymana przez Zamawiającego po terminie składania ofert zostanie niezwłocznie zwrócona Wykonawcy.

## 7. OPIS SPOSOBU UDZIELANIA WYJAŚNIEŃ DOTYCZĄCYCH TREŚCI ZAPYTANIA OFERTOWEGO, INFORMACJA O SPOSOBIE POROZUMIEWANIA SIĘ Z WYKONAWCAMI ORAZ SPOSOBIE PRZEKAZYWANIA OŚWIADCZEŃ I DOKUMENTÓW

7.1 Wykonawca może do dnia **06.03.2026** zwrócić się do Zamawiającego z prośbą o wyjaśnienie treści ZO. Zamawiający niezwłocznie nie później niż do dnia **09.03.2026** prześle odpowiedzi do wszystkich zaproszonych Wykonawców/zamieści odpowiedź na zapytania na swojej stronie internetowej: www.spzoz.lukow.pl (w zakładce: „zamówienia do 130000")

7.2Zamawiający wyznacza do kontaktowania się z Wykonawcami nw. osobę/y: Tomasz Buziak, t.buziak@spzoz.lukow.pl

7.3 Oświadczenia, wnioski, zawiadomienia oraz inne informacje mogą być przekazywane przez strony za pomocą e-maila.

## 8. MIEJSCE I TERMIN OTWARCIA OFERT

8.1 Oferty zostaną otwarte w siedzibie Zamawiającego przy ul. Partyzantów 10, pok. Nr 18, w dniu **10.03.2026**, o godzinie **11:00.**

**8.2** Otwarcie **ofert jest jawne**.

## 9. KRYTERIA WYBORU OFERTY NAJKORZYSTNIEJSZEJ

1.1. Ocena ofert będzie dokonana w oparciu o następujące kryteria:

**cena oferty brutto** - 100 %

W kryterium „cena oferty brutto" ocena ofert zostanie dokonana przy zastosowaniu wzoru:

$$\text{liczba punktów oferty ocenianej} = \frac{\text{najniższa cena oferty brutto}}{\text{cena oferty ocenianej brutto}} \times 100$$

**1.2.** Wszystkie obliczenia zostaną dokonane z dokładnością do dwóch miejsc po przecinku.

## 10. UNIEWAŻNIENIE POSTĘPOWANIA

Zamawiający unieważni postępowanie w przypadku gdy:

- żadna z ofert nie będzie spełniać wymogów określonych w ZO,
- cena najkorzystniejszej oferty przekroczy wartość, jaką zamawiający może przeznaczyć na finansowanie zamówienia.

Zamawiający zastrzega sobie możliwość unieważnienia postępowania bez podania przyczyny.

## 11. UDZIELANIE ZAMÓWIENIA

11.1 Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w niniejszym ZO i stanowi ofertę najkorzystniejszą z punktu widzenia przyjętych kryteriów.

11.2 Wzór umowy stanowi **Załącznik nr 2** do Zapytania ofertowego.

## 12. OPIS SPOSOBU OBLICZENIA CENY OFERTY

12.1. Cena oferty zostanie wyliczona przez Wykonawcę i przedstawiona w formularzu specyfikacji cenowej (**Załącznik Nr 1 do formularza oferty**).

12.2. Przy sporządzaniu oferty Wykonawca uwzględnia wszystkie wymogi, o których mowa w niniejszym ZO i ujmuje wszelkie koszty związane z wykonywaniem przedmiotu zamówienia, niezbędne dla prawidłowego i pełnego wykonania przedmiotu zamówienia.

## 13. OCHRONA DANYCH OSOBOWYCH

.....

## 14. INFORMACJA

W związku z wymogami art. 24 oraz art. 25 Ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Łukowie wdrożono PROCEDURĘ DOKONYWANIA ZGŁOSZEŃ NARUSZEŃ PRAWA I PODEJMOWANIA DZIAŁAŃ NASTĘPCZYCH, zawierającą:

1. rodzaje naruszeń prawa podlegające zgłoszeniom w SPZOZ w Łukowie;
2. osoby odpowiedzialne za przyjmowanie zgłoszeń wewnętrznych;
3. zasady zgłaszania informacji o naruszeniach prawa i podejmowania działań następczych;
4. warunki objęcia ochroną sygnalistów zgłaszających informacje o naruszeniach prawa;
5. środki ochrony sygnalistów;
6. tryb dokonywania zgłoszeń zewnętrznych.

Pełna treść wyżej wymienionego dokumentu dostępna jest w siedzibie SPZOZ w Łukowie.

**Załącznik nr 1 do ZO**

(Pieczęć Wykonawcy)

# OFERTA

## Dla: Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Łukowie

Nawiązując do Zapytania ofertowego nr **ZO/SI/1/2026**

na: **Szkolenia kadry kierowniczej i personelu z zakresu cyberbezpieczeństwa**

zgodnie z wymaganiami określonymi w ZO,
My niżej podpisani:

Nazwa Wykonawcy: .....
Adres:.....
Tel./fax. :.....
REGON:.....
NIP:.....

1. SKŁADAMY OFERTĘ na wykonanie przedmiotu zamówienia zgodnie z zapisami ZO
2. OŚWIADCZAMY, że zapoznaliśmy się z zapisami Zapytania ofertowego oraz wyjaśnieniami i zmianami przekazanymi przez Zamawiającego w trakcie postępowania i uznajemy się za związanych określonymi w nich postanowieniami i zasadami postępowania.
3. ZOBOWIĄZUJEMY SIĘ do wykonywania zamówienia przez okres .....od daty zawarcia umowy za cenę jednostkową (brutto), określoną na piśmie w załączniku do niniejszej oferty,
4. AKCEPTUJEMY warunki płatności określone przez Zamawiającego w ZO.
5. UWAŻAMY SIĘ za związanych niniejszą ofertą przez czas wskazany w ZO, tj. przez okres 30 dni od upływu terminu składania ofert.
6. OŚWIADCZAMY, że zapoznaliśmy się z Istotnymi dla stron postanowieniami umowy/wzorem umowy, określonymi w ZO i zobowiązujemy się w przypadku wyboru naszej oferty, do zawarcia umowy zgodnej z niniejszą ofertą, na warunkach określonych w ZO, w miejscu i terminie wyznaczonym przez Zamawiającego.
7. Uprawnionym do kontaktów z Zamawiającym jest ..... tel. .....fax.....e-mail:.....
8. Oświadczamy, że zawarty w specyfikacji projekt umowy został przez nas zaakceptowany i w przypadku wyboru naszej oferty zobowiązujemy się do zawarcia umowy na wyżej wymienionych warunkach, w miejscu i w czasie wyznaczonym przez zamawiającego,
9. Oświadczamy, że nie zachodzą w stosunku do nas przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. *o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego* (Dz. U. 2024.507 tj. ze zm.).[1]

---

[1] Zgodnie z treścią art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. *o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego,* z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp wyklucza się:
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 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2023 r. poz. 1124 t.j.) 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 2022 r., 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;

10. Załącznikami do niniejszej oferty są :
    1. .....str.....
    2. .....str.....
    3. .....str.....
    4. .....str.....

.....,dnia.....20..... r. .....

(podpis Wykonawcy lub osób upoważnionych do występowania w imieniu Wykonawcy)

3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120 t.j.), 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 2022 r., 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.

Załącznik nr 1 do formularza oferty

(Pieczęć Wykonawcy)

# FORMULARZ SPECYFIKACJI CENOWEJ

Przystępując do udziału w postępowaniu o udzielenie zamówienia publicznego nr **ZO/SI/1/2026** na: **Szkolenia kadry kierowniczej i personelu z zakresu cyberbezpieczeństwa**, przeprowadzonym w trybie Zapytania Ofertowego, oferujemy wykonanie przedmiotu zamówienia w oparciu o następujące ceny:

| Lp. | Asortyment* ..... | Ilość | Cena jedn. netto | Wartość netto (3x4) | Vat (od wartości netto) | Wartość brutto ogółem |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| **RAZEM** | | | | | | |

*zakres usługi, numer katalogowy lub inna cecha oferowanego produktu pozwalająca na jego identyfikację

....,dnia.....20.... r. .....

(podpis Wykonawcy lub osób upoważnionych do występowania w imieniu Wykonawcy)

**Załącznik nr 3 do ZO**

# ZAKRES PRZEDMIOTU ZAMÓWIENIA

**Zadanie 1.**

Przeprowadzenie szkolenia kadry kierowniczej zamawiającego obejmującego swoim zakresem następujące zagadnienia:

1) Zakres przedmiotowy i podmiotowy obowiązywania przepisów dotyczących cyberbezpieczeństwa.
2) Obowiązki podmiotów publicznych, w tym jednostek ochrony zdrowia.
3) Obowiązki podmiotu publicznego medycznego uznanego za operatora usługi kluczowej.
4) Struktura krajowego systemu cyberbezpieczeństwa.
5) Zadania i rola CSIRT NASK - Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego.
6) Wymagania prawne oraz znaczenie Systemu Zarządzania Bezpieczeństwem Informacji w organizacji.
7) Definicje i przykłady incydentów cyberbezpieczeństwa
8) Obsługa incydentów cyberbezpieczeństwa.
9) Wymagania dyrektywy NIS2 w obszarze cyberbezpieczeństwa i jej implementacja.
10) Rodzaje ataków **omówienie, przykłady oraz konsekwencje**:
    - ataki socjotechniczne (phishing i jego rodzaje, Watering Hole, Baiting, Scareware, Deepfake );
    - ataki na systemy i sieci (DDoS, Brute Force Attack, ataki na aplikacje webowe, ataki na urządzenia IoT, inżynieria wsteczna);
    - ataki Ransomware;
    - ataki na tożsamość;
    - wirusy – metodyka działania i metody ochrony.
11) AI - krótkie wprowadzenie do sztucznej inteligencji i przykłady jak może być wykorzystywana przeciwko nam.
12) HTTPS – dlaczego nie http.
13) WPA2 – dlaczego już nie jest bezpieczne.
14) Cała prawda o VPNach - czym są, co zapewniają a czego nie.
15) Kody QR.
16) MitM - nie tylko WiFi można podsłuchiwać
17) Zabezpieczenie informatycznych nośników danych – pendrivy i pamięci zewnętrzne.
18) Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia.
19) Przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych.
20) Prawidłowe korzystanie z oprogramowania antywirusowego.

21) Zasady aktualizacji programów i aplikacji.
22) Szyfrowanie dokumentów i poczty elektronicznej.
23) Polityka haseł, zarządzanie dostępem i tożsamością.

**Zadanie 2.**
Przeprowadzenie szkolenia pracowników administracji oraz pracowników medycznych zamawiającego obejmującego swoim zakresem następujące zagadnienia:

1) Obowiązki podmiotów publicznych, w tym jednostek ochrony zdrowia.
2) Obowiązki podmiotu publicznego medycznego uznanego za operatora usługi kluczowej.
3) Zadania i rola CSIRT NASK - Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego.
4) Definicje i przykłady incydentów cyberbezpieczeństwa
5) Obsługa incydentów cyberbezpieczeństwa.
6) Wymagania dyrektywy NIS2 w obszarze cyberbezpieczeństwa i jej implementacja.
7) Rodzaje ataków **omówienie, przykłady oraz konsekwencje**:
    - ataki socjotechniczne (phishing i jego rodzaje, Watering Hole, Baiting, Scareware, Deepfake );
    - ataki na systemy i sieci (DDoS, Brute Force Attack, ataki na aplikacje webowe, ataki na urządzenia IoT, inżynieria wsteczna);
    - ataki Ransomware;
    - ataki na tożsamość;
    - wirusy – metodyka działania i metody ochrony
8) AI - krótkie wprowadzenie do sztucznej inteligencji i przykłady jak może być wykorzystywana przeciwko nam.
9) HTTPS – dlaczego nie http
10) WPA2 – dlaczego już nie jest bezpieczne
11) Cała prawda o VPNach - czym są, co zapewniają a czego nie.
12) Kody QR.
13) MitM - nie tylko WiFi można podsłuchiwać
14) Zabezpieczenie informatycznych nośników danych – pendrivy i pamięci zewnętrzne.
15) Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia.
16) Przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych.
17) Prawidłowe korzystanie z oprogramowania antywirusowego.
18) Zasady aktualizacji programów i aplikacji.
19) Szyfrowanie dokumentów i poczty elektronicznej.
20) Polityka haseł, zarządzanie dostępem i tożsamością.

**Zadanie 3.**
Dostęp do platformy szkoleniowej dla 1000 pracowników, przedstawiającej tą samą tematykę jak w zadaniu 1 i 2.
Certyfikaty ukończenia szkolenia, dla każdego pracownika.