Białystok, 14.07.2026 r.

INF/10/2026/MD

**Zaproszenie do złożenia oferty**

Uniwersytecki Dziecięcy Szpital Kliniczny im. L. Zamenhofa w Białymstoku, ul. J. Waszyngtona 17, zwraca się z prośbą o złożenie oferty na **Wykonanie audytu końcowego w zakresie cyberbezpieczeństwa w Uniwersyteckim Dziecięcym Szpitalu Klinicznym im. L. Zamenhofa w Białymstoku**

## I. Opis przedmiotu zamówienia:

1. Wynik audytu: dokument potwierdzający poziom bezpieczeństwa systemów teleinformatycznych wykorzystywanych do udzielania świadczeń opieki zdrowotnej.
2. Dokumenty odniesienia/kryteria oceny:
   - Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. (Dz.U. 2024 poz. 773),

     https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20240000773
   - Regulaminem wyboru przedsięwzięcia do objęcia wsparciem w ramach krajowego planu odbudowy i zwiększania odporności Inwestycja D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia" będąca elementem komponentu D „Efektywność, dostępność i jakość systemu ochrony zdrowia". Nabór nr KPOD.07.03-IP.10-001/25,

     https://www.gov.pl/attachment/9fe55093-6182-47f7-b671-6de549e87bb6
   - Dokumentacja systemu zarządzania przedsiębiorstwa
3. Audyt będzie obejmował obszary, w których przetwarzane są dane osobowe wrażliwe, w tym kluczowe systemy informacji medycznej oraz infrastrukturę urządzeń medycznych (aparatura medyczna wraz z systemami je obsługującymi). Audyt będzie obejmował niezbędną infrastrukturę teleinformatyczną podmiotu:
   - Kanały komunikacji jak np. poczta
   - Sieciowe urządzenia brzegowe wraz z zasadami segmentacji oraz przepływów
   - Kontrolery domeny
   - Platformy wirtualizacyjne
   - Systemy zarządzania kopiami zapasowymi
   - Poprawność konfiguracji stacji roboczych oraz serwerów
   - Sposoby uwierzytelniania się użytkowników
4. Zakres audytu, kryteria i sposób dokumentowania w odniesieniu do ankiety weryfikacji dojrzałości w zakresie cyberbezpieczeństwa zgodnie z Regulaminem wyboru przedsięwzięcia do objęcia wsparciem w ramach krajowego planu odbudowy i zwiększania odporności Inwestycja D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony

zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia" będąca elementem komponentu D „Efektywność, dostępność i jakość systemu ochrony zdrowia". Nabór nr KPOD.07.03-IP.10-001/25.

5. Metodyka audytu:
   - Obserwacje audytora (np. wizja lokalna stref bezpieczeństwa fizycznego, wykaz aktywów, ustawienia systemu są odpowiednie),
   - Wywiad z personelem/kontrahentami nt. procesów i zabezpieczeń,
   - Przegląd wyników działania zabezpieczeń oraz analiza dokumentów (np. wydruk praw dostępu, zapisy z rozwiązania incydentu, przegląd logów z wykonywanych kopii bezpieczeństwa, analiza procedury incydentów etc),
   - Testowanie zabezpieczeń przez audytora (np. próba wykonania zadania otwarcia drzwi kartą gościa, ustalenie czy baza wirusów jest aktualna, prośba o weryfikację procedury bezpiecznego logowania).
6. Wymagania audytorów:
   - zgodnie z załącznikiem 2 Zarządzenia Nr 8/2023/BBIICD Prezesa określone w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. (Dz.U. poz. 1999) w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu lub jednostkę oceniająca zgodność, akredytowana zgodnie z przepisami ustawy z dnia
   - 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854 z późn.zm.), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych.
   - Audytor musi posiadać jeden z certyfikatów, takich jak np. CISA (Certified Information Systems Auditor), CISSP (Certified Information Systems Security Professional), czy certyfikaty audytora wiodącego ISO 27001.
7. Audyt zostanie wykonany po realizacji zadań:
   - Rozbudowa i integracja systemu szpitalnego o możliwość elektronicznego podpisu dokumentów za pomocą urządzeń do zbierania podpisu wraz z wymaganymi licencjami i sprzętem.
   - Rozbudowa systemu laboratoryjnego o generowanie dokumentów zgodnych z PIK Hl7 CDA i przekazywanie do repozytorium w HIS
   - Obsługa serwisowa systemu laboratoryjnego na 36 miesięcy od dnia wdrożenia
   - Rozbudowa systemu CIS o dodatkowe licencje Elektronicznej Karty Znieczulenia (EKZ)
   - Gwarancja i obsługa systemu CIS 3 lata od dnia wdrożenia
   - Rozbudowa posiadanego przez Szpital systemu do obsługi procesu sterylizacji moduł do ewidencji oznakowanych narzędzi
   - Obsługa serwisowa posiadanego przez Szpital zintegrowanego z HIS systemu do obsługi procesu sterylizacji na 36 miesięcy
   - Obsługa serwisowa posiadanego przez Szpital systemu HIS wraz z tworzeniem i wysyłaniem EDM do P1 na 36 miesięcy
   - Rozszerzenia EDM do 9 nowych dokumentów dla systemu HIS
   - Rozszerzenia EDM o moduł karty szczepień wraz z pełną integracją z P1
   - Zakup serwera obliczeniowego dla usług szpitalnych (3 sztuki)

- Licencje wirtualizatora (6 sztuk)
- Licencje systemu Windows Serwer 2025 (6 sztuk)
- Komputery all-in-one wraz z oprogramowaniem biurowym (85 sztuk)
- Wymiana systemu PACS - licencja, wdrożenie i wsparcie
- Zakup skanera z podajnikiem poziomym do digitalizacji dokumentów (2 sztuki)
- Zakup modułu do HIS do digitalizacji papierowej dokumentacji medycznej wraz z wdrożeniem
- System kopii zapasowych: deduplikator typu All-Flash z wbudowanym oprogramowaniem do wykonywania kopii zapasowych oraz oprogramowaniem do ochrony przed ransomware'em
- System kopii zapasowych: usługa wdrożenia, wsparcia i szkolenia (20 godzin)
- Zapora sieciowa: zakup zapory sieciowej klasy UTM (2 sztuki)
- Zapora sieciowa: usługa wdrożenia i wsparcia UTM wraz ze szkoleniem z obsługi
- Segmentacja sieci: zakup przełączników sieciowych wraz z niezbędnymi modułami optycznymi (45 sztuk)
- Segmentacja sieci: usługa wdrożenia, wsparcia i szkolenia
- Ochrona stacji roboczych oraz serwerów: licencja systemu XDR/EDR dla zwiększenia bezpieczeństwa ochrony urządzeń końcowych (900 licencji)
- Ochrona stacji roboczych oraz serwerów - usługa wdrożenia, wsparcia i szkolenia
- Przygotowanie dokumentacji pod wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji
- Szkolenie w zakresie cyberbezpieczeństwa dla personelu szpitala
- Szkolenie w zakresie cyberbezpieczeństwa dla kardy kierowniczej i działu IT
- Usługi zarządzane bezpieczeństwa: rozszerzenie ilości licencji do zarządzania IT (300 licencji)
- Usługi zarządzane bezpieczeństwa: umowa serwisowa na oprogramowanie do zarządzania IT na 3 lata
- Migracja z niewspieranych systemów operacyjnych, na których pracują HIS, PACS i e-Usługi na aktualne i wspierane systemy operacyjne
- Uwierzytelnienie i autoryzacja do systemów: licencja systemu PAM dla kontroli dostępu użytkowników z uprawnieniami administratora (50 sztuk)
- Uwierzytelnienie i autoryzacja do systemów: usługa wdrożenia, wsparcia oraz szkolenie do licencji systemu PAM dla kontroli dostępu użytkowników z uprawnieniami administratora
- Integracja z Platformą Usług Inteligentnych (PUI) - licencja wraz z wdrożeniem

**II. Oferta ma zawierać:**

1. Nazwę oraz adres kontaktowy
2. Informację, czego dotyczy

3. Kwotę netto PLN, kwotę brutto PLN oraz stawkę podatku VAT w %
4. Kwota podana w ofercie powinna zawierać wszystkie koszty Wykonawcy związane z realizacją przedmiotu zamówienia, niezbędne dla prawidłowego i pełnego jego wykonania oraz uwzględniać wszelkie opłaty, a także podatki wynikające z realizacji zamówienia, jak również ewentualne upusty i rabaty skalkulowane przez Wykonawcę.

## III. Termin złożenia oferty:

Ofertę należy złożyć do 20.07.2026 r. do godz. 15:00 drogą mailową na adres md@udsk.pl

1. Kryterium oceny oferty: 100% cena
2. Osoba kontaktowa: Michał Dojlido tel. 501515712 md@udsk.pl
3. Termin związania ofertą wynosi 7 dni od upływu terminu składania ofert.

## V. Termin realizacji zamówienia:

Do 11.08.2026 r.