Załącznik nr 1
do Zapytania ofertowego w celu oszacowania wartości zamówienia

OPIS PRZEDMIOTU ZAMÓWIENIA

DOTYCZY:
Usługi wykonania audytu końcowego w obszarze cyberbezpieczeństwa zgodnie z wymaganiami określonymi poniżej realizowanej w ramach inwestycji D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia" Krajowego Planu Odbudowy i Zwiększania Odporności.
Audyt powinien obejmować przynajmniej 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 powinien obejmować niezbędną infrastrukturę teleinformatyczną podmiotu, w tym przynajmniej bezpieczeństwo takich elementów jak:

- Kanały komunikacji jak np. poczta
- Sieciowe urządzenia brzegowe wraz z zasadami segmentacji oraz przepływów
- Kontrolery domeny
- Platforma wirtualizacyjna
- System zarządzania kopiami zapasowymi
- Poprawność konfiguracji stacji roboczych oraz serwerów
- Sposoby uwierzytelniania się użytkowników

Obecnie Zamawiający posiada aktualne certyfikaty:

1) Systemu zarządzania bezpieczeństwem informacji na zgodność z normą PN-ISO/IEC 27001:2023:
   Data pierwszej certyfikacji: 5.11.2018
2) Systemu zarządzania jakością na zgodność z normą ISO 9001:2015:
   Data pierwszej certyfikacji: 28.09.2011
3) Akredytacyjny Ministra Zdrowia z dnia 30.12.2025.

W ramach zawartej umowy Wykonawca:

1. Przeprowadzi Audyt końcowy w obszarze cyberbezpieczeństwa w siedzibie Zamawiającego w terminie uzgodnionym z Zamawiającym, jednak nie później niż do 25.05.2026
2. Audyt przeprowadzony zostanie przez Zespół audytujący: co najmniej dwóch audytorów posiadających certyfikaty określone w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. (Dz.U. poz. 1999) w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu lub co najmniej dwóch audytorów posiadających co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych lub jednostka 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.
3. Audyt zostanie przeprowadzony zgodnie z regulaminem naboru w ramach inwestycji D.1.1.2. „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia" Krajowego Planu Odbudowy i Zwiększania Odporności (KPO) dostępnym na stronie https://www.gov.pl/web/zdrowie/inwestycja-d112-przyspieszenie-procesow-transformacji-cyfrowej-ochrony-zdrowia-poprzez-dalszy-rozwoj-uslug-cyfrowych-w-ochronie-zdrowia-nabor-konkurencyjny
4. Minimalny zakres audytu i kryteria akceptacji stosowane podczas audytu końcowego w obszarze cyberbezpieczeństwa obejmują:
   - System kopii zapasowych
   - Zapory sieciowe
   - Ochrona poczty e-mail
   - Segmentacja sieci
   - Ochrona stacji roboczych oraz serwerów (rozwiązania klasy EDR)
   - Zarządzanie podatnościami
   - System zarządzania bezpieczeństwem informacji
   - Szkolenia z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa

(cyberhigieny)
- Usługi zarządzane bezpieczeństwem
- Uwierzytelnienie i autoryzacja do systemów

5. Po zakończeniu Audytu jednostka przedstawi Zamawiającemu wyniki Audytu Końcowego w obszarze cyberbezpieczeństwa, w postaci pisemnego raportu.
6. Raport musi zawierać minimum:
    - opis zakresu i metodologii audytu,
    - ocenę zgodności projektu z KPO D.1.1.2,
    - przedstawienie porównania poziomu Cyberbezpieczeństwa w stosunku do dokonanej przez Zamawiającego samooceny poziomu dojrzałości Cyberbezpieczeństwa, która była przeprowadzona na etapie składania wniosku o objęcie przedsięwzięcia wsparciem ze środków KPO sformułowanie wniosków po wykonanym audycie szczególnie w zakresie poziomu Cyberbezpieczeństwa w stosunku do pierwszej Ankiety weryfikacji dojrzałości pod kątem Cyberbezpieczeństwa
7. Raport musi być sporządzony w języku polskim
8. Jednostka certyfikująca zachowa poufność wszelkich otrzymanych od Zamawiającego informacji.
9. Szczegółowo przebieg usługi zostanie określony w Umowie.