Załącznik nr 1 do zapytania ofertowego DNIT.230.89.2026

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest wykonanie usługi polegającej na przeprowadzeniu audytu bezpieczeństwa, zgodnie z wymaganiami określonymi w kryteriach akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa.

Zamówienie realizowane w ramach projektu pn.”*Wdrożenie cyfrowych rozwiązań dla poprawy jakości, dostępności i bezpieczeństwa danych medycznych w Szpitalu Uniwersyteckim w Krakowie.”* współfinansowanego z **Krajowego Planu Odbudowy i Zwiększania Odporności (KPO)**. 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”.

1. Sposób realizacji prac.

1) Audyt końcowy w obszarze cyberbezpieczeństwa musi obejmować ocenę podmiotu co najmniej na poziomie pozytywnym lub warunkowo pozytywnym, w oparciu o kryteria wskazane w *Ankiecie weryfikacji dojrzałości w zakresie cyberbezpieczeństwa,* obejmujące:
   a) kryteria obligatoryjne,
   b) kryteria nieobligatoryjne, wskazane przez Zamawiającego we wniosku o objęcie przedsięwzięcia wsparciem
2) Wypełniona *Ankieta weryfikacji dojrzałości w zakresie cyberbezpieczeństwa* zostanie przekazana Wykonawcy wyłonionemu w ramach niniejszego postępowania.
3) Zakres audytu powinien obejmować w szczególności obszary, w których przetwarzane są dane osobowe wrażliwe, w tym:
   a) systemy informacji medycznej,
   b) infrastrukturę urządzeń medycznych, w tym aparaturę medyczną wraz z systemami ją obsługującymi.
4) Audyt powinien obejmować niezbędną infrastrukturę teleinformatyczną podmiotu, w tym przynajmniej bezpieczeństwo takich elementów jak:
   a) kanały komunikacji jak np. Poczta
   b) sieciowe urządzenia brzegowe wraz z zasadami segmentacji oraz przepływów
   c) kontrolery domeny
   d) platformy wirtualizacyjne
   e) systemy zarządzania kopiami zapasowymi
   f) poprawność konfiguracji stacji roboczych oraz serwerów
   g) sposoby uwierzytelniania się użytkowników
5) Zamawiający rekomenduje, aby Wykonawca przy realizacji audytu wykorzystał kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa, określone w *Załączniku nr 4 do Regulaminu – Zakres realizacji przedsięwzięcia,* dostępnego na stronie Ministerstwa Zdrowia https://www.gov.pl/web/zdrowie/inwestycja-d112-przyspieszenie-procesow-transformacji-cyfrowej-ochrony-zdrowia-poprzez-dalszy-rozwoj-uslug-cyfrowych-w-ochronie-zdrowia-nabor-konkurencyjny?fbclid=IwY2xjawM3JXhleHRuA2FlbQIxMAABHurxbzO8yyZx4JudmsuxBy2-2giRBejqv3Zb6mONGHgqzwkj4lmV3Bn44Gu6_aem_Eomh71r80gctf3-8E-zkvQ
6) Wykonawca zobowiązany jest do realizacji przedmiotu zamówienia zgodnie z zasadą „nie czyń poważnych szkód” (DNSH – Do No Significant Harm), o której mowa w art. 17 Rozporządzenia

Parlamentu Europejskiego i Rady (UE) 2020/852, mającej zastosowanie do przedsięwzięć finansowanych w ramach Krajowego Planu Odbudowy i Zwiększania Odporności (KPO). Szczegółowe wymagania w tym zakresie określa załącznik nr 2 do zapytania ofertowego.

2. Wymagania dla członków zespołu audytowego.

1) Zamawiający wymaga, aby w realizacji zamówienia uczestniczył zespół audytowy posiadający odpowiednie kwalifikacje i doświadczenie.
2) Warunek ten uznaje się za spełniony, jeżeli Wykonawca zapewni:
   a) 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
   b) co najmniej dwóch audytorów posiadających co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych
   lub
   c) realizację zamówienia przez 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.
3) Zamawiający dopuszcza łączne spełnienie powyższych wymagań przez zespół Wykonawcy, przy czym jedna osoba może spełniać więcej niż jedno z powyższych kryteriów.
4) W celu potwierdzenia spełnienia powyższych wymagań Wykonawca zobowiązany jest do przedłożenia wraz z ofertą wykazu osób wraz z załączoną dokumentacją spełnienia wymagań.

3. Oczekiwany produkt finalny.

1) Produktem końcowym realizacji zamówienia będzie raport z audytu końcowego w obszarze cyberbezpieczeństwa, zawierający w szczególności:
   a. ocenę poziomu dojrzałości cyberbezpieczeństwa Zamawiającego,
   b. ocenę zgodności z kryteriami określonymi w *Ankiecie weryfikacji dojrzałości,*
   c. jednoznaczne wskazanie stopnia spełnienia kryteriów obligatoryjnych oraz nieobligatoryjnych,
   d. wnioski z przeprowadzonego audytu.
2) Raport stanowić będzie podstawę do rozliczenia projektu w ramach Krajowego Planu Odbudowy i Zwiększania Odporności (KPO).