Załącznik nr 2 do zapytania

Wykonanie audytu końcowego w obszarze cyberbezpieczeństwa

Przedmiotem zamówienia jest wykonanie audytu bezpieczeństwa zgodnie z wymaganiami określonymi w kryteriach akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa w ramach inwestycji D.1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia".

Celem audytu końcowego jest potwierdzenie spełnienia kryteriów akceptacji w obszarze cyberbezpieczeństwa określonych dla Inwestycji D.1.1.2, w tym uzyskanie co najmniej oceny pozytywnej lub warunkowo pozytywnej, zgodnie z Ankietą weryfikacji dojrzałości w zakresie cyberbezpieczeństwa stanowiącą podstawę samooceny Zamawiającego na etapie składania wniosku o objęcie przedsięwzięcia wsparciem.

Wykonawca audytu zobowiązany jest do przedstawienia wyników audytu w formie tabelarycznej, zawierającej:
- odniesienie do każdego kryterium Ankiety weryfikacji dojrzałości w zakresie cyberbezpieczeństwa,
- wskazanie statusu: spełnione /niespełnione /spełnione warunkowo,
- krótkie, jednoznaczne uzasadnienie dokonanej oceny.

Audyt obejmuje wykonanie testów bezpieczeństwa o charakterze weryfikacyjnym, mających na celu potwierdzenie skuteczności wprowadzonych zabezpieczeń oraz zgodności konfiguracji systemów z dokumentacją powykonawczą, zgodnie z kryteriami akceptacji Inwestycji D.1.1.2.
Testy te nie mają charakteru testów penetracyjnych ani testów inwazyjnych i nie obejmują prób omijania zabezpieczeń, wykorzystywania podatności, symulacji ataków ani działań mogących powodować zakłócenia pracy systemów produkcyjnych, o ile Zamawiający nie zleci ich odrębnie.

W ramach realizacji audytu Wykonawca dostarczy:
- raport główny z audytu,
- mapowanie wyników audytu do kryteriów Ankiety weryfikacji dojrzałości,
- ocenę końcową audytu (pozytywna/ warunkowo pozytywna),
- plan działań naprawczych lub doskonalących - jeżeli dotyczy,
- oświadczenie potwierdzające zgodność przeprowadzonego audytu z wymaganiami Inwestycji D.1.1.2

Audyt powinien obejmować niezbędną infrastrukturę teleinformatyczną podmiotu, w tym przynajmniej bezpieczeństwo takich elementów jak:
- Bezpieczeństwo kanałów komunikacji (np. poczta elektroniczna),
- Sieciowe urządzenia brzegowe wraz z zasadami segmentacji oraz przepływów,
- Kontrolery domeny i ich konfigurację,
- Platforma wirtualizacyjna oraz jej zabezpieczenia,
- System zarządzania kopiami zapasowymi,
- Poprawność konfiguracji stacji roboczych oraz serwerów,
- Sposoby uwierzytelniania się użytkowników.

Audyt musi zostać wykonany w terminie od momentu podpisania umowy **do dnia 10.07.2026r**., bądź w innym terminie uzgodnionym przez Strony liczonym od daty powiadomienia Wykonawcy o możliwości przystąpienia do realizacji zamówienia. Termin określony w ten sposób uzasadniony jest od konieczności wykonania pozostałych zamówień, które zostaną zrealizowane przed możliwością jego rozpoczęcia. Powiadomienie nastąpi na adres mailowy wskazany w Umowie.

Audyt realizowany będzie przez zespół audytujący składający się z 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 przy czym, co najmniej jeden audytor powinien posiadać minimum 3-letnie doświadczenie w obszarze bezpieczeństwa informacji.