Załącznik do formularza oferty

**Zadanie nr 14 - Audyt końcowy w zakresie cyberbezpieczeństwa i testy bezpieczeństwa**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametry techniczne i funkcjonalne** | **Wymagania graniczne** | **Parametry oferowane**  *(podać zakres lub opisać)* |
| **Audyt końcowy w zakresie cyberbezpieczeństwa i testy bezpieczeństwa, w skład którego wchodzi:** | | | |
| **I.**  **Wykonanie audytu końcowego 1 - szt.** | | | |
|  | Nazwa: | Podać |  |
|  | Wykonawca | Podać |  |
|  | Kraj pochodzenia | Nd. |  |
|  | Rok produkcji nie starszy niż 2025, urządzenie fabrycznie nowe | Nd. |  |
|  | Wynik audytu:  dokument potwierdzający poziom bezpieczeństwa systemów teleinformatycznych wykorzystywanych do udzielania świadczeń opieki zdrowotnej. | TAK/Podać |  |
|  | 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), * 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, * Dokumentacja systemu zarządzania przedsiębiorstwa. | TAK |  |
|  | 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 | TAK |  |
|  | Zakres audytu, kryteria i sposób dokumentowania zgodnie z Załącznikiem nr 3 do Wniosku o objęcie przedsięwzięcia wsparciem Ankieta 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. | TAK |  |
|  | 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). | TAK |  |
|  | 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. | TAK / Podać |  |
|  | Audyt zostanie wykonany po realizacji zadań z pakietów od 1 do 13 oraz 15 i Punktu II w Pakiecie 14 | TAK |  |
|  | Sporządzenie raportu końcowego – maksimum 5 dni po zakończeniu audytu, | TAK/Podać |  |
|  | Rozpoczęcie audytu minimum 7 dni od zgłoszenia gotowości przez Zamawiającego do wykonania audytu. Maksimum 10 dni. | TAK/Podać |  |
| **II.**  **Testy bezpieczeństwa systemów IT - 1 - szt.** | | | |
|  | Nazwa: | Podać |  |
|  | Wykonawca | Podać |  |
|  | Kraj pochodzenia | Nd. |  |
|  | Rok produkcji nie starszy niż 2025, urządzenie fabrycznie nowe | Nd. |  |
|  | Zakres prac:  Testy bezpieczeństwa będą obejmować wybrane obszary, w których przetwarzane są dane osobowe wrażliwe, w tym kluczowe systemy informacji medycznej. Audyt będzie obejmować niezbędną infrastrukturę teleinformatyczną podmiotu, w tym przynajmniej bezpieczeństwo takich elementów jak:   * Usługi i infrastruktura podmiotu dostępne z Internetu * Infrastruktura sieci wewnętrznej podmiotu * Usługa katalogowa * Platforma wirtualizacyjna * Kanały komunikacji - serwery odpowiedzialne za świadczenie usługi poczty elektronicznej * Poprawność konfiguracji wybranej próbki serwerów oraz stacji roboczych. | TAK |  |
|  | Audyt poprawności konfiguracji:   * Sieciowe urządzenia brzegowe wraz z zasadami segmentacji oraz przepływów * Kontrolery domeny * System zarządzania kopiami zapasowymi | TAK |  |
|  | Raport dla każdej z usług będzie wyszczególniać zakres przeprowadzonych testów lub audytu oraz wszystkie  wyniki ze szczególnym uwzględnieniem potencjalnych skutków wpływu zmaterializowania się zagrożenia,  wskazanie środków, które wpłyną na poprawę stanu zabezpieczenia systemu oraz szczegóły techniczne  wykrytych podatności i nieprawidłowości konfiguracyjnych wraz z określeniem poziomu ich istotności. | TAK /Podać |  |

……………………………….

(podpis/popisy osoby/osób upoważnionej/upoważnionych

do reprezentowania wykonawcy)