

Specyfikacja zamówienia 19/IT/2023

Budowa kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji, w celu zapewnienia bezpieczeństwa informacji i bezpieczeństwa cybernetycznego Uniwersyteckiego Centrum Klinicznego Warszawskiego Uniwersytetu Medycznego, uwzględniającego wymogi ustawowe związane z OUK i ustawą o KSC i jej akty wykonawcze.

Przedmiot zamówienia obejmuje działania zmierzające do wdrożenia wymagań Ustawy o krajowym systemie cyberbezpieczeństwa (KSC) w sposób kompleksowy. Zamówienie obejmuje realizację następujących po sobie czynności tj.:

1. audyt zero (sprawdzenie stanu obecnego) wraz z rekomendacjami,
2. analizę wpływu i szacowanie ryzyka wraz z rekomendacjami,
3. sporządzenie dokumentacji systemu zarządzania bezpieczeństwem informacji wraz z dostosowaniem obecnych procesów lub ich ponownego zaprojektowania do specyfikacji jednostki Zamawiającego,
4. szkolenia personelu

Powyższe czynności mają za zadanie przygotowania jednostki do pomyślnej realizacji audytu bezpieczeństwa systemu informacyjnego zgodnie z Ustawą z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa wraz z jej aktami wykonawczymi zgodnie z decyzją Ministerstwa Zdrowia z dnia 14 lipca 2022 roku o uznaniu UCK WUM za Operatora Usług Kluczowych i w tym kontekście będą prowadzone.

Wyłonienie jednego wykonawcy do realizacji tych czynności pozwoli na zachowanie ich spójności i przyczyni się do doboru właściwych metod prac wdrożeniowych, celem osiągnięcia podniesienia poziomu cyberbezpieczeństwa w całej organizacji. Pozwoli to na zoptymalizowanie działań i dobór właściwych metod. Wykonawca będzie odpowiedzialny kompleksowo za osiągnięcie oczekiwanych rezultatów. Ułatwi to również porozumiewanie się i koordynację prac pomiędzy uczestnikami procesu, co przyczyni się do obniżenia kosztów logistycznych oraz związanych ze zaznajomieniem się przez wykonawcę z funkcjonującym i oczekiwanym systemem u Zamawiającego.

Należy również zaznaczyć iż Uniwersyteckie Centrum Kliniczne Warszawskiego Uniwersytetu Medycznego (dalej UCK WUM) posiada trzy zakłady lecznicze takie jak: Centralny Szpital Kliniczny (dalej CSK) przy ulicy Banacha 1a w Warszawie, Dziecięcy Szpital Kliniczny (dalej DSK) przy ulicy Żwirki i Wigury 63A w Warszawie, oraz Szpital Kliniczny Dzieciątka Jezus (dalej SKDJ) przy ulicy Lindleya 4 w Warszawie. UCK WUM zostało uznane za operatora usług kluczowych (dalej OUK) polegających na:

- udzielaniu świadczeń opieki zdrowotnej przez podmiot publiczny,
- obrocie i dystrybucji produktów leczniczych.

I. Opis przedmiotu zamówienia

1. Przedmiot zamówienia

Przedmiotem zamówienia jest wykonanie usługi polegającej na

- a. Przeprowadzenie audytu zerowego stwierdzającego obecny stan przygotowania Systemu SZBI Zamawiającego lub jego elementów do wymogów ustawy o KSC i jej aktów wykonawczych.
- b. Przeprowadzenie Analizy Ryzyka wystąpienia incydentu.
- c. Opracowaniu dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (dalej SZBI) w UCK WUM będącego Operatorem Usług Kluczowych (dalej OUK) wraz z przekazaniem praw autorskich wytworzonej na te potrzeby dokumentacji zgodnie z wymaganiami ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.

U. z 2021 r. poz. 2070 ze zm.), rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 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. z 2017 r. poz. 2247), oraz ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z 2021 r. poz. 2333 i 2445 oraz z 2022 r. poz. 655);

- d. Przygotowanie szkoleń dla personelu Zamawiającego z SZBI.
 - e. Realizacja szkolenia stacjonarnego dla Kadry Zarządzającej Zamawiającego z SZBI (20 osób).
2. Termin realizacji zamówienia wynosi 60 dni od daty podpisania umowy. Wykonawca w ciągu 3 dni po podpisaniu umowy przedstawi Zamawiającemu propozycję harmonogramu zawierającego ramy czasowe dla każdego z 4 punktów szczegółowego opisu przedmiotu zamówienia.

II. Szczegółowy opis przedmiotu zamówienia

1. Przeprowadzenie Audytu zerowego

Wykonawca określi na podstawie tzw. audytu zerowego stan przygotowania jednostki oraz jego dokumentacji i procesów do realizacji wymagań określonych w:

- a. Ustawie o KSC z dnia 5 lipca 2018 r.
- b. rozporządzeniach wykonawczych, zwłaszcza Rozporządzeniu Ministra Cyfryzacji z dnia 4 grudnia 2019 r w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo
- c. normie PN-ISO/IEC 27001
- d. normie PN-ISO/IEC 22301

i przedstawi rekomendacje przygotowania lub aktualizacji niezbędnej dokumentacji oraz zmian w procesach realizowanych w UCK WUM.

2. Przeprowadzenie analizy ryzyka

Wykonawca dokona analizy ryzyka wystąpienia incydentu w UCK WUM jako OUK i przedstawi raport z przeprowadzonej analizy wraz z rekomendacjami oraz opisem zastosowanej metodologii szacowania ryzyka.

3. Wykonanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji

Wykonawca, na podstawie wymagań określonych w:

- a. Ustawie o KSC,
- b. rozporządzeniach wykonawczych, zwłaszcza Rozporządzeniu Ministra Cyfryzacji z dnia 4 grudnia 2019 r w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwa,
- c. normie PN-ISO/IEC 27001
- d. normie PN-ISO/IEC 22301

oraz na podstawie rekomendacji zawartych w wynikach przeprowadzonego audytu zerowego i testów penetracyjnych oraz przeprowadzonej analizy ryzyka wystąpienia incydentu przedstawi propozycję kompletnej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, przy uwzględnieniu istniejących dokumentów w UCK WUM, które będą włączone do dokumentacji SZBI. Kompletna dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji będzie dodatkowo przekazana w postaci dokumentów edytowalnych (np. docx, xlsx).

4. Przygotowanie szkoleń dla personelu Zamawiającego

- a. W celu zaznajomienia personelu Zamawiającego z Systemem Zarządzania Bezpieczeństwem Informacji który zostanie dostarczony przez Wykonawcę, niezbędne będzie przeprowadzenie dedykowanych szkoleń. Szkolenia muszą zostać podzielone zgodnie z kompetencjami personelu Zamawiającego na grupy: personel biały, pracownicy administracji, pracownicy Działu Informatyki, oraz Zarząd UCK WUM.
- b. Szkolenia zostaną przeprowadzone w formie online jako prezentacja zakończona testem.
- c. Testy będą sprofilowane dla 4 grup wskazanych w punkcie 1 osobno i będzie można wybrać do której grupy należą.
- d. Szkolenia będą zrealizowane przez Wykonawcę w formie umożliwiającej uruchomienie ich na platformie szkoleniowej Moodle Zamawiającego.
- e. Dalsze opieka nad frekwencją rozwiązywanych testów będzie po stronie Zamawiającego. Dostarczenie i prawidłowe uruchomienie szkoleń na platformie Moodle będzie świadczyło o realizacji zadania.
- f. Prawa autorskie do materiałów i szkoleń będą przekazane Zamawiającemu zgodnie z Rozdział I. punkt 1 d
 - a. Realizacja szkolenia stacjonarnego dla Kadry Zarządzającej Zamawiającego z SZBI.

W celu zaznajomienia personelu Zamawiającego z Systemem Zarządzania Bezpieczeństwem Informacji który zostanie dostarczony przez Wykonawcę, niezbędne będzie przeprowadzenie szkolenia stacjonarnego dla Kadry Zarządzającej do 20 osób.

III. Wymogi co do realizacji przedmiotu zamówienia

1. W związku z tym, że przedmiot zapytania musi być realizowany przez podmiot spełniający warunki z art. 15 pkt 2 UKSC Zamawiający prosi o zawarcie w ofercie informacyjnej oświadczenia, że Państwa zespół wdrożeniowy posiada:
 - a) co najmniej 4 audytorów z ważnymi certyfikatami określonymi w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. (poz. 1999) w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu bezpieczeństwa,
 - b) każdy z audytorów posiada co najmniej pięcioletnią praktykę w zakresie wdrożenia systemu zarządzania bezpieczeństwem informacji zgodnie z PN-ISO/IEC 27001 lub systemu zarządzania ciągłością działania opartą PN-ISO/IEC 22301
 - c) przeprowadził co najmniej 5 audytów w jednostkach będących operatorami usługi kluczowej zgodnie z UKSC
 - d) co najmniej 4 audytorów dysponujących odpowiednim doświadczeniem do wykonania zamówienia, warunek ten zostanie spełniony, jeżeli Wykonawca wykaże, że w okresie trzech ostatnich lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie wykonał, a w przypadku świadczeń okresowych lub ciągłych wykonuje co najmniej 4 zamówienia u podmiotów zatrudniających co najmniej 1000 pracowników każdy, z których każde polegało/polega na wsparciu przy doskonaleniu lub wdrożeniu Systemów Zarządzania Bezpieczeństwem Informacji w oparciu o normę PN-ISO/IEC 27001:2017
 - e) aktualną polisę OC w zakresie prowadzonej działalności w wysokości min. 1 000 000 PLN.osoby zdolne (minimum 5 osób) (z certyfikatami określonymi w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. (poz. 1999)) do wykonania zamówienia, którzy posiadają aktualny certyfikat audytora wiodącego Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z normą PN-ISO/IEC 27001 (min. 4 osoby).