##### Szkolenia z zakresu podnoszenia świadomości w obszarze Cyberbezpieczeństwa wraz z Opracowaniem Systemu Zarządzania Bezpieczeństwem Informacji (SzBI)

Przedmiotem zamówienia jest przeprowadzenie szkolenia w obszarze Cyberbezpieczeństwa dla pracowników WCSKJ **(Pakiet Nr 1)** wraz z opracowaniem i wdrożeniem Systemu Zarządzania Bezpieczeństwem Informacji (SzBI) opartym o wymagania normy ISO/IEC 27001:2022 **(Pakiet Nr 2)**.

System ma obejmować całość działalności medycznej, administracyjnej i technicznej, dokumentacji medycznej (EDM) systemów teleinformatycznych oraz infrastruktury krytycznej w rozumieniu ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC). System ma być kompatybilny z obowiązującym u Zamawiającego systemem ochrony danych osobowych.

##### Zakres zamówienia

**Pakiet Nr 1**

Przeprowadzenie szkolenia z zakresu podniesienia świadomości w obszarze Cyberbezpieczeństwa z dostosowaniem do różnych grup odbiorców, od ogółu pracowników po specjalistów IT i kadrę zarządzającą. Kluczowe jest skupienie się na najnowszych zagrożeniach, takich jak phishing, ransomware oraz ataki socjotechniczne, a także na praktycznych sposobach ochrony danych, w tym tworzeniu silnych haseł i zasadach bezpiecznego korzystania z technologii.

Szkolenie powinno obejmować zarówno aspekty techniczne, jak i behawioralne, a jego celem jest minimalizacja ryzyka incydentów bezpieczeństwa i zapewnienie zgodności z

##### Wymagania dotyczące wykonawcy

Pakiet Nr 1

W celu potwierdzenia spełnienia warunku zdolności technicznej lub zawodowej Zamawiający uzna warunek za spełniony, jeżeli Wykonawca wykaże, że trener w ciągu  
ostatnich 3 lat przeprowadził min. 10 dni szkoleniowych z zakresu cyberbezpieczeństwa, a  
szkolenia były realizowane w ciągu 2 różnych lat kalendarzowych. W celu potwierdzenia  
spełnienia warunku w Wykazie osób skierowanych do realizacji zlecenia należy podać termin  
realizacji usługi oraz posiada minimum 1 certyfikat wskazany w wykazie certyfikatów uprawniających do przeprowadzenia audytu (Załącznik do rozporządzenia Ministra Cyfryzacji z dnia 12.10.2018 do ustawy o KSC).

W celu potwierdzenia spełnienia warunku zdolności technicznej lub zawodowej Wykonawca w Wykazie zrealizowanych usług zobowiązany jest podać przedmiot wykonanej usługi, datę rozpoczęcia i zakończenia usługi, podmiot, na rzecz którego wykonywał usługę.

Powyższe warunki będą weryfikowane na podstawie złożonego przez Wykonawcę wykazu zrealizowanych usług wraz z załączeniem dokumentów potwierdzających wykonanie usług.

Zamawiający uzna warunek za spełniony, jeżeli Wykonawca potwierdzi, że skieruje do realizacji usługi 1-ną osobę (trenera) posiadającą co najmniej 2-letnie doświadczenie w zakresie prowadzenia szkoleń budujących i wzmacniających świadomość cyberzagrożeń.

**Zamawiający wymaga zawarcia umowy o Poufności oraz umowy powierzenia przetwarzania danych na wzorze udostępnianym przez Zamawiającego.**

**Wymagania formalne**

* Realizacja zadania w terminie do 15.05.2026 r.;

**Wymagania dotyczące rezultatów**

* Przeszkolenie wszystkich pracowników WCSKJ z potwierdzeniem wiedzy (np. test końcowy);
* Identyfikacji kontekstu funkcjonowania organizacji w obszarze SZBI, pracownicy muszą rozumieć, dlaczego bezpieczeństwo jest ważne akurat w ich specyficznej pracy. Szkolenie powinno wskazać konkretne aktywa informacyjne (dane pacjentów, dokumentacja techniczna) oraz zagrożenia specyficzne dla Naszej branży;
* Zakres odpowiedzialności w obszarze SZBI. Pracownik musi wiedzieć, co mu wolno, a czego nie i kto odpowiada za dany proces.;

**Pakiet Nr 2**

Opracowanie dokumentacji SZBI opartej o wymagania normy ISO/IEC 27001:2022

* Opracowanie Polityki Bezpieczeństwa Informacji;
* Opracowanie procedur w obszarach: klasyfikacja informacji, incydenty, kopie zapasowe, zarządzanie ryzykiem oraz podatnościami w zakresie Cyberbezpieczeństwa, dostęp do danych, ciągłość działania – kompatybilne z obowiązującymi procedurami ochrony danych osobowych lub zaproponowanie zmian;
* Opracowanie Polityki Logowania Zdarzeń z uwzględnieniem aplikacji, sieci, serwerów, bram brzegowych, kontrolerów domeny;
* Opracowanie   
  Polityki Kryptografii z uwzględnieniem zalecanych dopuszczalnych protokołów szyfrowania;
* Opracowania Polityki realizacji kopii bezpieczeństwa;
* Opracowanie procedur audytu wewnętrznego systemu SZBI;
* Opracowanie rejestru ryzyka, planów postępowania z ryzykiem, planu ciągłości działania i planu odtwarzania po awarii, zarządzania ciągłością działania;

##### Wymagania dotyczące wykonawcy

Pakiet Nr 2

W celu potwierdzenia spełnienia warunku zdolności technicznej lub zawodowej Zamawiający wymaga, aby Wykonawca przystępujący do zapytania wykazał, ze posiada minimum 3-letnie doświadczenie w zakresie opracowywania i wdrażania systemów zarządzania bezpieczeństwem informacji (SZBI) oraz opracowywania i wdrażania systemów zarządzania ochroną danych osobowych. Co najmniej 3 wdrożenia SZBI w podmiotach medycznych, publicznych lub prywatnych.

W celu potwierdzenia spełnienia warunku zdolności technicznej lub zawodowej Zamawiający uzna warunek za spełniony, jeżeli Wykonawca wykaże, że w ciągu ostatnich 3 lat, a jeśli okres działalności jest krótszy to w tym okresie, zrealizował 3 usługi polegające na opracowaniu wdrożenia SZBI.

W celu potwierdzenia spełnienia warunku Wykonawca w Wykazie zrealizowanych usług zobowiązany jest podać przedmiot wykonanej usługi, datę rozpoczęcia i zakończenia usługi, podmiot, na rzecz którego wykonywał usługę.

Powyższe warunki będą weryfikowane na podstawie złożonego przez Wykonawcę wykazu zrealizowanych usług wraz z załączeniem dokumentów potwierdzających wykonanie usług.

Zamawiający wymaga aby Zespół Wdrożeniowy Wykonawcy składał się z:

* Audytora wiodącego ISO 27001 lub odpowiednich kwalifikacji;
* Ekspert do spraw RODO (posiadający praktykę w pracy z podmiotami medycznymi, z doświadczeniem pełnienia funkcji IOD w podmiocie medycznym);
* Specjalistę ds. Cyberbezpieczeństwa.

**Zamawiający wymaga zawarcia umowy o Poufności oraz umowy powierzenia przetwarzania danych na wzorze udostępnianym przez Zamawiającego.**

Wykonawca musi posiadać Polisę OC na kwotę min. 1 000 000 zł .

Wymagania dotyczące rezultatów

* Opracowanie dokumentacji SZBI opartej o wymagania normy ISO/EC 27001:2022 kompletna dokumentacja (WORD/EXCEL), zgodnie z zakresem zamówienia określonym w Zakresie zamówienia;
* Identyfikacji kontekstu funkcjonowania organizacji w obszarze SZBI;
* Zakres odpowiedzialności w obszarze SZBI;
* Identyfikacja aktywów przetwarzających informacje oraz ocena ich wartości;
* Opracowanie macierzy ryzyka, opracowanie analizy ryzyka oraz planu postępowania z ryzykiem;
* Procedury działań korygujących oraz plan audytów wewnętrznych SZBI;
* Opracowanie deklaracji stosowania SZBI;

##### Wymagania formalne

* Realizacja zadania w terminie do 15.05.2026 r.;
* Konsultacje online w trakcie opracowywania dokumentacji.

…………………………………………………………………………………………………

***Dokument należy podpisać podpisem elektronicznym: kwalifikowanym, zaufanym lub osobistym bądź wydrukowany dokument podpisać własnoręcznie, zeskanować - załączyć do oferty poprzez Bazę Konkurencyjności***