

Szczegółowy Opis Przedmiotu Zamówienia

Spis treści

Spis treści	1
1. Wprowadzenie	1
2. Przedmiot i cel zamówienia	1
2.1. Przedmiot zamówienia	1
2.2. Cel zamówienia	2
3. Etapy i zakres realizacji usług	2
3.1. Etap 1 - Analiza ryzyka i audyt obszaru bezpieczeństwa informacji	2
3.2. Etap 2 - Opracowanie i przekazanie pełnej dokumentacji systemu SZBI	3
3.3. Etap 3 - Szkolenia personelu związane z wdrożeniem oraz stosowaniem SZBI	4
4. Terminy, zasady i warunki realizacji Przedmiotu Zamówienia	5
4.1. Terminy realizacji prac, odbiór oraz wymagania stawiane Wykonawcy	5
4.2. Warunki realizacji usług szkoleniowych	6
4.3. Wsparcie wdrożenia ze strony Zamawiającego	7

1. Wprowadzenie

Zamówienie realizowane jest w ramach projektu pn. „Rozwój cyfryzacji i cyberbezpieczeństwa w Szpitalu w Krynicy-Zdroju”, objętego wsparciem z Krajowego Planu Odbudowy i Zwiększania Odporności, inwestycja D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia”, nabór nr KPOD.07.03-IP.10-001/25.

Zakres przedmiotu zamówienia jest zgodny z dokumentacją inwestycji KPO dostępną na stronie internetowej [inwestycji D.1.12](#).

2. Przedmiot i cel zamówienia

2.1. Przedmiot zamówienia

Przedmiotem zamówienia jest opracowanie dokumentacji i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w SPZOZ Szpitalu im. dr. J. Dietla w Krynicy-Zdroju.

Przedmiot zamówienia obejmuje opracowanie dokumentacji i wdrożenie kompletnego Systemu Zarządzania Bezpieczeństwem Informacji uwzględniającego kontekst organizacyjny Zamawiającego, w celu osiągnięcia zgodności funkcjonowania Szpitala z wymogami:

- Polskiej Normy PN-EN ISO/IEC 27001, ISO/IEC 27002 i ISO/IEC 27005
- rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI),
- ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC), z uwzględnieniem jej aktualnych oraz potencjalnych zmian legislacyjnych w okresie realizacji zamówienia,

- przepisów ustawy o ochronie danych osobowych i rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO),

w zakresie obejmującym co najmniej procesy i usługi świadczone przez Zamawiającego. Zamówienie obejmuje również analizę ryzyka i audyt obszaru bezpieczeństwa oraz przeszkolenie personelu związane z wdrożeniem oraz stosowaniem udokumentowanego SZBI. Zamawiający nabywa pełne autorskie prawa majątkowe do opracowanej dokumentacji SZBI z prawem do jej dalszej modyfikacji i dostosowywania do zmian organizacyjnych i prawnych.

Zakres i realizacja Przedmiotu Zamówienia przebiegać będzie z podziałem na 3 etapy:

- **Etap 1:** Analiza ryzyka i audyt obszaru bezpieczeństwa informacji.
- **Etap 2:** Opracowanie, przekazanie i wdrożenie pełnej dokumentacji systemu SZBI.
- **Etap 3:** Szkolenie personelu związane z wdrożeniem oraz stosowaniem SZBI.

Szczegółowy zakres zamówienia został omówiony w rozdziale 3.

2.2. Cel zamówienia

Celem realizacji zamówienia jest zwiększenie zgodności procesów, systemów i procedur funkcjonujących w SPZOZ Szpitalu im. dr J. Dietla w Krynicy-Zdroju z krajowymi i unijnymi wymogami w zakresie bezpieczeństwa informacji, w tym:

- a) ustanowienie i wdrożenie skutecznego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnego z obowiązującymi w tym zakresie przepisami i normami;
- b) przygotowanie oraz wzmocnienie kompetencji zespołu ds. bezpieczeństwa informacji;
- c) zwiększenie poziomu cyberbezpieczeństwa Szpitala w zakresie organizacyjnym i technicznym;
- d) zapewnienie zgodności z wymogami ustawy o Krajowym Systemie Cyberbezpieczeństwa, z uwzględnieniem jej aktualnych oraz projektowanych nowelizacji;
- e) przygotowanie jednostki do audytu bezpieczeństwa potwierdzającego zabezpieczenie przetwarzania Elektronicznej Dokumentacji Medycznej (EDM), zgodnie z wymaganiami inwestycji KPO D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia” (wskaźnik D21G.R2).

3. Etapy i zakres realizacji usług

3.1. Etap 1 - Analiza ryzyka i audyt obszaru bezpieczeństwa informacji.

1. Wykonawca dokona analizy stanu obecnego technicznego i organizacyjnego, w tym posiadanej przez Zamawiającego dokumentacji oraz analizy ryzyk związanych z przetwarzaniem informacji i funkcjonowaniem systemów informatycznych, w tym infrastruktury medycznej i administracyjnej.
2. Wykonawca przeprowadzi **szczegółową analizę ryzyka informacji** w środowisku Szpitala wraz z inwentaryzacją aktywów (w tym w szczególności aktywów IT) związanych z przetwarzaniem informacji i ich klasyfikacją oraz opracuje **rekomendacje działań mitygujących zidentyfikowane ryzyka**.
3. Wykonawca wykona **audyt obszaru bezpieczeństwa** informacji obejmującego:
 - a) Klasyfikacja podmiotu względem ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (t.j. Dz.U. 2024, poz. 1077, z późn.zm.) z uwzględnieniem wymagań projektowanych w nowelizacji tejże ustawy, które zostałyby wprowadzone najnowszym dostępnym projektem ustawy o zmianie ustawy o Krajowym Systemie

Cyberbezpieczeństwa oraz niektórych innych ustaw
(<https://legislacja.gov.pl/projekt/12384504>) (dalej „UKSC2”).

- b) Analiza stanu gotowości podmiotu względem UKSC2;
 - c) Przegląd istniejącej dokumentacji i procesów w obszarze bezpieczeństwa informacji oraz stosowanych zabezpieczeń bezpieczeństwa informacji, procesów zarządzania ryzykiem i audytowania względem wymagań polskich norm PN-EN ISO/IEC 27001, PN-EN ISO/IEC 27002, PN-EN ISO/IEC 27005;
 - d) Przegląd obecnej dokumentacji i procesów w obszarze ciągłości działania, względem wymagań polskich norm PN-EN ISO 22301, PN-EN ISO 22313;
 - e) Przegląd obecnej dokumentacji w obszarze Ochrony Danych Osobowych względem ustawy RODO;
 - f) Przegląd polityki tworzenia i testowania kopii zapasowych względem rekomendacji Ministerstwa Zdrowia oraz rekomendacji Centrum e-Zdrowia;
 - g) Przegląd stosowanych w Szpitalu rozwiązań zabezpieczeń;
 - h) Badanie zgodności dokumentacji i procesów w obszarze bezpieczeństwa informacji względem Rozporządzenia 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 (dalej „Rozporządzenie KRI”).
 - i) **Przegląd bezpieczeństwa IT** obejmujący co najmniej następujące obszary:
 - i. infrastruktura sieciowa: weryfikacja zabezpieczeń dostępu zewnętrznego do sieci, weryfikacja aktualności oprogramowania sprzętu sieciowego oraz ocena podatności sprzętowych i softwarowych, weryfikacja dostępu do sieci Wi-Fi (szyfrowanie, kontrola dostępu, segmentacja),
 - ii. serwery i systemy: ocena aktualności systemów operacyjnych i oprogramowania serwerowego, sprawdzenie sposobu tworzenia, przechowywania i zabezpieczenia kopii bezpieczeństwa,
 - iii. stacje robocze i środowisko użytkowników: weryfikacja dostępu do stacji roboczych w sieci LAN, sprawdzenie aktualności oprogramowania, systemów operacyjnych i zabezpieczeń lokalnych.
4. Wykonawca przedstawi wyniki analizy ryzyka i audytu oraz sporządzone w oparciu o niego rekomendacje w postaci jednolitego i spójnego raportu wraz z załączonymi wynikami szczegółowymi poszczególnych badań oraz opracowań zrealizowanych w ramach audytu.

3.2. Etap 2 - Opracowanie i przekazanie pełnej dokumentacji systemu SZBI

1. Wykonawca przy współudziale Zamawiającego dokona:

- a) opracowania i aktualizacji dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) z elementami ciągłości działania w bezpieczeństwie informacji w oparciu o normę **ISO 22301**, uwzględniający kontekst organizacyjny Zamawiającego, w celu osiągnięcia zgodności z polskimi normami **PN-EN ISO/IEC 27001, PN-EN ISO/IEC 27002 i ISO/IEC 27005**, Rozporządzeniem **KRI, UKSC2** oraz **RODO**, jak również zgodnie z wymaganiami inwestycji **KPO D1.1.2** (Załącznik nr 4 do Regulaminu naboru). Wsparcie dotyczy w szczególności opracowania, uzupełnienia, aktualizacji lub integracji dokumentacji w zakresie bezpieczeństwa informacji:
 - 1) Metodyka identyfikacji, szacowania i postępowania z ryzykiem;
 - 2) Analiza ryzyka;
 - 3) Polityka bezpieczeństwa informacji;
 - 4) Deklaracja stosowania ISO 27001;
 - 5) Polityka bezpieczeństwa organizacyjnego;

- 6) Polityka bezpieczeństwa systemów teleinformatycznych;
- 7) Polityka bezpieczeństwa pracowniczego;
- 8) Polityka bezpieczeństwa fizycznego i środowiskowego;
- 9) Polityka ochrony danych osobowych;
- 10) Analiza BIA;
- 11) Polityka ciągłości działania;
- 12) Wymagane polityki, procedury, regulaminy i instrukcje niższego poziomu powiązane z w/w dokumentami, w szczególności polityki określone w wymogach inwestycji KPO:
 - a. Polityka zarządzania dostępem i uprawnieniami;
 - b. Polityka kryptografii z uwzględnieniem zalecanych dopuszczalnych protokołów szyfrowania;
 - c. Politykę zarządzania ryzykiem z uwzględnieniem obszaru cyberbezpieczeństwa;
 - d. Politykę logowania zdarzeń z uwzględnieniem aplikacji, sieci, serwerów, bramy brzegowej, kontrolerem domeny;
 - e. Politykę kopii bezpieczeństwa;
 - f. Politykę zarządzania incydentami bezpieczeństwa;
 - g. Politykę zarządzania ciągłością działania;
 - h. Politykę ochrony danych osobowych z uwzględnieniem przetwarzania danych medycznych;
 - i. Procedury eksploatacyjne systemów bezpieczeństwa IT.
- b) przeglądu i aktualizacji polityk ochrony danych osobowych oraz uzupełnienia brakującej dokumentacji ochrony danych osobowych pod kątem integracji i dostosowania do wymogów SZBI i RODO;
- c) wsparcia we wdrożeniu opracowanej dokumentacji i procedur w organizacji szpitala;
- d) wsparcia w określeniu ról i utworzeniu wewnętrznej struktury organizacyjnej bezpieczeństwa informacji (m.in. wyznaczenie Pełnomocnika ds. SZBI, Administratorów bezpieczeństwa, Zespołu reagowania na incydenty);
- e) wsparcia w implementacji procedur zarządzania ryzykiem, incydentami i ciągłością działania;
- f) Wykonawca zapewni wsparcie doradcze i konsultacje w zakresie wdrożenia polityk technicznych bezpieczeństwa, w tym opracowanie rekomendacji konfiguracyjnych dla istniejących systemów zabezpieczeń, bez wykonywania zmian konfiguracyjnych w środowisku produkcyjnym.
- g) Wykonawca przygotowuje listę wymagań związanych z bezpieczeństwem informacji oraz listę środków technicznych dla zapewnienia bezpieczeństwa informacji z uwzględnieniem środków aktualnie wykorzystywanych przez Zamawiającego

3.3. Etap 3 - Szkolenia personelu związane z wdrożeniem oraz stosowaniem SZBI

1. Wykonawca zapewni szkolenia dla kadry zarządzającej oraz Zespołu odpowiedzialnego za bezpieczeństwo powołanego w przebiegu realizacji wdrożenia, związane z wdrożeniem oraz stosowaniem udokumentowanego SZBI obejmujące w szczególności:
 - a) zasady funkcjonowania SZBI oraz stosowanie opracowanych polityk i procedur bezpieczeństwa informacji,
 - b) role, obowiązki i odpowiedzialność członków zespołu ds. bezpieczeństwa informacji,
 - c) proces przeglądu zarządczego SZBI, w tym cykl aktualizacji i doskonalenia systemu,
 - d) proces zarządzania ryzykiem, incydentami i ciągłością działania,
 - e) prowadzenie i aktualizacja rejestrów bezpieczeństwa informacji oraz dokumentowanie działań i incydentów,

- f) wymogi raportowania oraz dokumentowania przeglądów SZBI sposoby
 - g) współpraca z personelem medycznym oraz Działem Informatyki w zakresie reagowania na incydenty bezpieczeństwa,
 - h) bezpieczeństwo informacji nieelektronicznych oraz przetwarzanych poza systemami teleinformatycznymi (bezpieczeństwo fizyczne),
 - i) omówienie obowiązujących regulacji, standardów, norm i dobrych praktyk w obszarze bezpieczeństwa teleinformatycznego, w tym: RODO, Dyrektywa NIS2, ustawa o Krajowym Systemie Cyberbezpieczeństwa, KRI, normy ISO/IEC 27001 i ISO 22301,
 - j) omówienie mechanizmów kontrolnych SZBI i Systemu Zarządzania Ciągłością Działania (SZCD),
 - k) rola kierownictwa w zapewnianiu i nadzorze nad bezpieczeństwem informacji oraz infrastrukturą krytyczną,
 - l) przegląd rozwiązań ochronnych, detekcyjnych i prewencyjnych w obszarze cyberbezpieczeństwa,
 - m) skuteczne reagowanie na incydenty oraz przywracanie ciągłości działania po ataku.
 - n) zasady przygotowania, prowadzenia i dokumentowania audytów wewnętrznych SZBI, w tym planowanie audytów, metodyka ich realizacji, raportowanie wyników oraz formułowanie działań korygujących.
2. Wykonawca przygotuje i dostarczy **materiały szkoleniowe** związane z wdrożeniem oraz stosowaniem udokumentowanego SZBI dla pozostałych pracowników Zamawiającego. Celem materiałów jest zapewnienie pracownikom możliwości szybkiego zapoznania się z wymaganiami wynikającymi z Polityk i Procedur SZBI oraz stosowania ich w codziennej pracy.

4. Terminy, zasady i warunki realizacji Przedmiotu Zamówienia

4.1. Terminy realizacji prac, odbiór oraz wymagania stawiane Wykonawcy

- 1. Wykonawca zrealizuje Przedmiot Zamówienia w zakresie i podziale na etapy określone szczegółowo w rozdziale 3.
- 2. Realizacja poszczególnych etapów będzie realizowana w następujących terminach:
 - a) **Etap 1** – do **35 dni** od dnia podpisania Umowy;
 - b) **Etap 2** – do **80 dni** od zakończenia Etapu 1;
 - c) **Etap 3** – do **15 dni** od zakończenia Etapu 2.
- 3. Każdy z etapów realizacji Przedmiotu Zamówienia, o których mowa w pkt 3, podlega odrębnemu odbiorowi przez Zamawiającego. Odbiór każdego etapu nastąpi na podstawie Protokołu Odbioru Częściowego, sporządzonego przez Strony i podpisanego bez zastrzeżeń.
- 4. Zamawiający zastrzega sobie prawo do wniesienia uwag do zawartości raportu z przeprowadzonego audytu bezpieczeństwa, do treści dokumentacji SZBI oraz materiałów szkoleniowych, zgłaszanych w trakcie procedury odbiorowej.
- 5. Po zakończeniu realizacji wszystkich etapów Przedmiotu Zamówienia, Strony podpiszą Protokół Odbioru Końcowego, który będzie stanowił podstawę do wystawienia przez Wykonawcę faktury VAT za wykonanie całości Przedmiotu Zamówienia.
- 6. System Zarządzania Bezpieczeństwem Informacji musi obejmować wszystkie zasoby informacyjne Szpitala, w tym: systemy medyczne (HIS, LIS, RIS, EDM), systemy administracyjne, serwery, urządzenia sieciowe, stacje robocze, systemy backupowe, infrastrukturę OT/IoMT (urządzenia medyczne podłączone do sieci) oraz dane przetwarzane poza systemami informatycznymi i procesy organizacyjne.
- 7. Wykonawca uwzględni w dokumentacji SZBI zmieniającą się infrastrukturę sprzętowo-systemową i zakupywane rozwiązania z zakresu cyberbezpieczeństwa w trakcie realizacji

Projektu pn. „Rozwój cyfryzacji i cyberbezpieczeństwa w Szpitalu w Krynicy-Zdroju” – dokonując odpowiednich korekt i uzupełnień w dokumentacji SZBI.

8. Wszystkie procedury i polityki muszą być opracowane w oparciu o **normy ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27005, ISO 22301**; ustawę o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. 2024 poz. 1077) z uwzględnieniem wymagań projektowanych w nowelizacji tejże ustawy, zgodnie z rozporządzeniem RODO, Rozporządzeniem KRI oraz wymaganiami KPO – inwestycja D1.1.2, wskaźnik D21G.R2.
9. Wykonawca do realizacji prac opisanych jako Etap 1 oraz Etap 2 skieruje zespół ekspertów składający się z co najmniej trzech audytorów/specjalistów spełniających warunki opisane w Zapytaniu ofertowym. Do realizacji Etapu 3 Wykonawca skieruje co najmniej jednego trenera, który posiada doświadczenie w przygotowywaniu i przeprowadzaniu szkoleń z zakresu zarządzania bezpieczeństwem informacji i/lub spełnia wymagania stawiane do realizacji Etapów 1 i 2.
10. Całościowy raport z audytu (Etap 1) wraz z wnioskami i zaleceniami oraz opracowany SZBI (Etap 2) zostaną podpisane przez certyfikowanego audytora uprawnionego do prowadzenia audytów zgodnie z Rozporządzeniem Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999).
11. Prace zostaną zrealizowane w trybie mieszanym tj. część prac (łącznie **minimum 10 dni** z pominięciem szkoleń) będzie realizowana w siedzibie Zamawiającego, a część zdalnie. Zamawiający dopuszcza wykonywanie prac w siedzibie Zamawiającego w dni robocze od poniedziałku do piątku w godzinach 8:00-14:30.

4.2. Warunki realizacji usług szkoleniowych

1. Szkolenia określone jako Etap 3 w rozdziale 3 zostaną zrealizowane w siedzibie Zamawiającego lub w trybie zdalnym za zgodą Zamawiającego.
2. Zamawiający dopuszcza możliwość podziału każdego szkolenia na 2 lub 3 sesje po uprzednim uzgodnieniu. Przewidywana łączna liczba godzin szkoleniowych nie powinna być krótsza niż 10 godzin.
3. Każdemu uczestnikowi szkoleń Wykonawca wystawi imienny certyfikat uczestnictwa.
4. Szkolenia, które będą przeprowadzone w placówce Zamawiającego muszą być realizowane w dni robocze w godzinach od 8:00 do 14:30.
5. Wykonawca jest zobowiązany przedstawić Zamawiającemu propozycję szczegółowego harmonogramu szkoleń nie później niż na 3 dni robocze przed planowanym rozpoczęciem szkoleń.
6. Wykonawca jest zobowiązany do uwzględnienia uwag przekazanych przez Zamawiającego, a w przypadku braku takiej możliwości, do przedstawienia nowej propozycji harmonogramu szkoleń w terminie maksymalnie 2 dni roboczych od przekazania uwag.
7. Wykonawca przygotuje i dostarczy materiały szkoleniowe związane z wdrożeniem oraz stosowaniem udokumentowanego SZBI dla pozostałych pracowników Zamawiającego. Celem materiałów jest zapewnienie pracownikom możliwości szybkiego zapoznania się z wymaganiami wynikającymi z Polityk i Procedur SZBI oraz stosowania ich w codziennej pracy.
8. Pod pojęciem „materiałów szkoleniowych” Zamawiający rozumie w szczególności:
 - prezentacje szkoleniowe (PPT/PDF) dotyczące zasad SZBI i obowiązków pracowników,
 - skrócone instrukcje / karty pracownika („one-pagery”) z kluczowymi zasadami bezpieczeństwa i zgłaszania incydentów,
 - checklisty dotyczące bezpiecznej pracy z systemami i danymi,
 - dokument podsumowujący SZBI dla pracowników.

Materiały mają umożliwić pracownikom szybkie zapoznanie się z zasadami SZBI i ich stosowanie w codziennej pracy.

9. Materiały szkoleniowe muszą być przygotowane w języku polskim, w formie elektronicznej, edytowalnej oraz w formie PDF.

4.3. Wsparcie wdrożenia ze strony Zamawiającego

1. Zamawiający umożliwi Wykonawcy prawidłowe wykonanie Przedmiotu Zamówienia, poprzez:
 - a) Udostępnienie lokalizacji na czas niezbędny do wykonania Przedmiotu Zamówienia.
 - b) Dostęp do wszelkich informacji i środków technicznych niezbędnych do realizacji Przedmiotu Zamówienia. Dostęp do informacji oznacza udostępnianie w postaci dokumentów papierowych lub elektronicznych dokumentacji i innych opracowań oraz informacji uzyskanych od pracowników Zamawiającego, które na podstawie uzasadnionego wniosku Wykonawcy mogą mieć wpływ na realizację Przedmiotu Zamówienia.
 - c) Wsparcie ze strony ustanowionego przez Zamawiającego zespołu składającego się z wyznaczonych przedstawicieli następujących jednostek: Działu Informatyki, Inspektora Ochrony Danych Osobowych.
 - d) Zamawiający wyznaczy pracownika odpowiedzialnego za współpracę z Wykonawcą oraz nadzór nad wdrożeniem.
2. W szczególności Zamawiający zobowiązuje się do:
 - a) Współpracy z Wykonawcą na każdym etapie realizacji Przedmiotu Zamówienia;
 - b) Udzielenia dostępu do dokumentacji i topologii infrastruktury sieciowej;
 - c) Udzielenia dostępu do raportów z dotychczas przeprowadzonych audytów;
 - d) Udzielenia dostępu do pełnomocników/koordynatorów ds. bezpieczeństwa, inspektora ochrony danych oraz administratorów systemów IT;
 - e) Użyczenie pomieszczenia w siedzibie Zamawiającego w celu prowadzenia szkoleń i badań audytowych przez zespół audytowy Wykonawcy.