Załącznik nr 1 do Zapytania Ofertowego

Opis Przedmiotu Zamówienia

Opracowanie dokumentacji SZBI oraz szkolenia w zakresie cyberbezpieczeństwa

Rudna Mała, październik 2025

# Informacje wstępne

Zamówienie niniejsze jest prowadzone w ramach projektu „Cyfryzacja i wzmocnienie cyberbezpieczeństwa podmiotu Nowe Techniki Medyczne Szpital Specjalistyczny im. Świętej Rodziny w Rudnej Małej. Nr wniosku KPOD.07.03-IP.10-0466/25” finansowanego ze środków Krajowego Planu Odbudowy i Zwiększania Odporności, Priorytet Efektywność, dostępność i jakość systemu ochrony zdrowia - część grantowa, Działanie D1.1.2. Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia, nr naboru: KPOD.07.03-IP.10-001/25

# Zakres zamówienia

Zakres niniejszego zamówienia obejmuje usługi w zakresie opracowanie dokumentacji SZBI oraz szkoleń dla pracowników Zamawiającego. Zamówienie obejmuje następujące elementy:

|  |  |  |
| --- | --- | --- |
| **Nazwa pozycji** | **Ilość** | **J,m.** |
| Przygotowanie, wdrożenie i utrzymanie systemu SZBI | 1 | Szt. |
| Szkolenia dla kadry kierowniczej z zakresu SZBI | 1 | Szt. |
| Szkolenia dla personelu medycznego i administracyjnego z SZBI | 1 | Szt. |

## Przygotowanie, wdrożenie i utrzymanie procedur związanych z SZBI

|  |
| --- |
| Celem zamówienia jest zaprojektowanie, udokumentowanie i wsparcie wdrożenia w strukturach Zamawiającego spójnego i funkcjonalnego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). System ten ma na celu zapewnienie poufności, integralności i dostępności informacji, a także osiągnięcie i utrzymanie zgodności z kluczowymi regulacjami prawnymi i normami.  **Kluczowe podstawy normatywne i prawne:**  Opracowany i wdrożony SZBI musi być w pełni zgodny z wymaganiami następujących dokumentów (w ich najnowszych, obowiązujących na dzień udzielenia zamówienia wersjach):   1. Norma ISO/IEC 27001 - "Information security, cybersecurity and privacy protection — Information security management systems — Requirements". 2. Norma ISO/IEC 27005 - "Information security, cybersecurity and privacy protection — Guidance on managing information security risks". 3. Norma ISO 22301 - "Security and resilience — Business continuity management systems — Requirements". 4. Norma PN-ISO/IEC 29134 – Wytyczne do przeprowadzenia oceny skutków dla prywatności (DPIA) 5. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. 6. Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (KRI). 7. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO). 8. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (Dyrektywa NIS 2).   W przypadku, gdy w trakcie realizacji zamówienia ww. akty prawne ulegną zmianie Wykonawca powinien przedstawić Zamawiającemu zakres niezbędnych zmian w zakresie aktualizacji przygotowanego SZBI. **Szczegółowy Zakres Prac** Realizacja zamówienia została podzielona na cztery logiczne, następujące po sobie etapy. Odbiór każdego etapu jest warunkiem koniecznym do rozpoczęcia kolejnego. **ETAP I: Audyt Zerowy i Analiza Luk**  1. **Przeprowadzenie diagnozy przedwdrożeniowej** w siedzibie Zamawiającego. 2. **Analiza dostępnej dokumentacji** wewnętrznej Zamawiającego (regulaminy, procedury, instrukcje) pod kątem ich wpływu na bezpieczeństwo informacji. 3. **Przeprowadzenie wywiadów** z kluczowym personelem (kadra zarządzająca, pracownicy IT, pracownicy medyczni i administracyjni) w celu zmapowania kluczowych procesów przetwarzania informacji. 4. **Weryfikacja i identyfikacja luk** w istniejących zabezpieczeniach (organizacyjnych, technicznych i fizycznych) w odniesieniu do każdego z wymagań aktów prawnych i norm wymienionych w pkt 2.2. 5. **Produkt/Deliverable:** Opracowanie i przekazanie Zamawiającemu **"Raportu z Audytu Zerowego"**, który musi zawierać:    * Streszczenie menedżerskie.    * Szczegółową analizę luk (Gap Analysis) z odniesieniem do konkretnych punktów norm i przepisów.    * Ocenę dojrzałości organizacji w obszarze bezpieczeństwa informacji.    * Rekomendacje działań naprawczych.    * Proponowany, zharmonizowany plan realizacji kolejnych etapów prac.  **ETAP II: Szacowanie i Analiza Ryzyka**  1. **Opracowanie i przedstawienie do akceptacji Zamawiającego metodyki analizy ryzyka**, zgodnej z normą ISO/IEC 27005. 2. **Wspólna z personelem Zamawiającego identyfikacja i inwentaryzacja aktywów** informacyjnych (dane, oprogramowanie, infrastruktura, ludzie). 3. **Klasyfikacja zidentyfikowanych aktywów** pod względem ich krytyczności (poufność, integralność, dostępność). 4. **Przeprowadzenie warsztatów szacowania ryzyka** z udziałem właścicieli procesów po stronie Zamawiającego, mających na celu identyfikację zagrożeń, podatności oraz ocenę poziomu ryzyka. 5. **Produkt/Deliverable:** Opracowanie i przekazanie Zamawiającemu kompletnej dokumentacji z analizy ryzyka, zawierającej:    * **Rejestr Aktywów Informacyjnych.**    * **Raport z Analizy Ryzyka**, zawierający zidentyfikowane ryzyka wraz z ich oceną.    * **Plan Postępowania z Ryzykiem**, określający sposób reakcji na każde zidentyfikowane ryzyko (akceptacja, mitygacja, transfer, unikanie).   Uwaga:  Wykonawca zobowiązany jest uwzględnić w planowanym szacowaniu, analizie i postępowaniu z ryzkami w zakresie bezpieczeństwa informacji, również specyfikę bezpieczeństwa danych osobowych i danych medycznych.  Metodyka analizy ryzyka zgodna z normą ISO/IEC 27005, winna obejmować również kryterium ryzyka w oparciu o przepisy RODO. W tym przypadku winny być uwzględnione ryzyka dla praw i wolności osób fizycznych, a następnie zaproponowanie w uzgodnieniu z Administratorem odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych osobowych.  Wymaganie powyższe wynika z interpretacji i oceny Prezesa UODO, który nałożył kare w wysokości 66 500 zł na Uniwersytecki Dziecięcy Szpital Kliniczny im. L. Zamenhofa w Białymstoku za niewdrożenie odpowiednich środków technicznych i organizacyjnych.  Prezes UODO zwrócił uwagę w opublikowanym komunikacie dotyczącym nałożonej kary, że istnieją różnice pomiędzy cyberbezpieczeństwem a ochroną danych osobowych. Administrator powołał się w tej sprawie na przeprowadzony audyt zgodności z ustawą o krajowym systemie cyberbezpieczeństwa. Organ nadzorczy wskazał, że – mimo pewnych podobieństw – procedury cyberbezpieczeństwa i ochrony danych osobowych służą różnym celom. Celem wdrażania procedur związanych cyberbezpieczeństwem jest przede wszystkim zapewnienie niezakłóconego i bezpiecznego świadczenia usług. Z kolei celem implementacji środków technicznych i organizacyjnych, o których mowa w RODO, jest zapewnienie bezpieczeństwa danym osobowym przetwarzanym przez Administratora. Spełnienie wymogów cyberbezpieczeństwa nie zawsze oznacza spełnienie wymogów ochrony danych. **ETAP III: Opracowanie Dokumentacji Systemowej SZBI**  1. Na podstawie wyników Etapu I i II, Wykonawca opracuje kompletny zestaw dokumentacji SZBI. 2. **Kluczowy wymóg:** Wszystkie dokumenty muszą być opracowane w ścisłej współpracy z Zamawiającym i w pełni **dostosowane do specyfiki jego działalności, procesów (medycznych i administracyjnych), zasobów oraz infrastruktury**. Niedopuszczalne jest dostarczenie generycznych, niezaadaptowanych szablonów. Akceptacja dokumentacji będzie uzależniona od wykazania, że odnosi się ona do realnych, nazwanych procesów, zasobów i ról funkcjonujących u Zamawiającego. 3. **Minimalny zakres dokumentacji:**    * Księga SZBI (podręcznik systemu).    * Polityka Bezpieczeństwa Informacji.    * Deklaracja Stosowania (SoA).    * Polityka Ochrony Danych Osobowych (zgodna z RODO).    * Polityki szczegółowe, zasady i procedury obejmujące m.in.:      + Zarządzanie aktywami.      + Bezpieczeństwo osobowe (cykl życia pracownika).      + Zarządzanie uprawnieniami i dostępem.      + Bezpieczeństwo fizyczne i środowiskowe.      + Bezpieczeństwo teleinformatyczne (sieci, systemy, aplikacje).      + Zarządzanie incydentami bezpieczeństwa informacji.      + Zarządzanie ciągłością działania.      + Zasady zgodności z wymaganiami prawnymi i umownymi.    * Polityki i szczegółowe zasady i procedury winny również uwzględnić takie dokumenty jak:      + Polityka klasyfikacji informacji,      + Polityka zarządzania dostępem i uprawnieniami,      + Polityka zarządzania podatnościami,      + Polityka zarządzania ryzykiem z uwzględnieniem obszaru cyberbezpieczeństwa i przetwarzania danych osobowych,      + Polityka zarządzania incydentami cyberbezpieczeństwa i danych osobowych,      + Polityka zarządzania ciągłością działania z uwzględnieniem Planu Ciągłości Działania (BCP) oraz Plan Odzyskiwania po Awarii (Disaster Recovery Plan - DRP),      + Polityka logowania zdarzeń z uwzględnieniem aplikacji, sieci, serwerów, bramy brzegowej, kontrolera domeny,      + Procedura zarządzania dostawcami (zarządzania łańcuchem dostaw),      + Procedura zarządzania zmianami w urządzeniach i systemach IT,      + Procedura zarzadzania pojemnością i wydajnością krytycznych zasobów teleinformatycznych,      + Procedura zarządzania dokumentacja i zapisami SZBI,      + Procedura audytów wewnętrznych SZBI.    * Inne dokumenty (instrukcje, regulaminy, wzory oświadczeń), których potrzeba opracowania zostanie zidentyfikowana i uzasadniona na podstawie wyników Etapu I i II, po obustronnym pisemnym zatwierdzeniu przez Zamawiającego i Wykonawcę. 4. **Produkt/Deliverable:** Kompletna, zatwierdzona przez Zamawiającego **dokumentacja SZBI** w edytowalnej formie elektronicznej (np. format .docx).   Dodatkowe wymagania i wyjaśnienia Zamawiającego:   1. Zamawiający informuje, że posiada opracowany Dokument Polityki Ochrony Danych (DPODO) Osobowych. Wykonawca zobowiązany jest uwzględnić zapisy tego dokumentu w przygotowanym SZBI i przygotować SZBI w taki sposób, aby zapisy Systemu nie spowodowały konieczności zmian w opracowanym DPODO.  **ETAP IV: Wsparcie Wdrożeniowe i Transfer Wiedzy**  1. **Przygotowanie dedykowanych materiałów szkoleniowych** dla różnych grup pracowników (kadra zarządzająca, personel IT, pracownicy medyczni, administracja). 2. **Aktywne wsparcie konsultacyjne i merytoryczne** dla zespołu Zamawiającego przy przeprowadzeniu pierwszego **audytu wewnętrznego SZBI**. 3. **Aktywne wsparcie konsultacyjne i merytoryczne** przy organizacji i przeprowadzeniu pierwszego **przeglądu zarządzania SZBI**. 4. **Produkt/Deliverable:**    * **Materiały szkoleniowe** w formie elektronicznej.    * **Protokół/raport z przeprowadzonych szkoleń** (zawierający program i listę uczestników).    * **Protokół/raport z audytu wewnętrznego** (opracowany wspólnie z zespołem Zamawiającego).    * **Protokół/raport z przeglądu zarządzania** (opracowany wspólnie z zespołem Zamawiającego).  **Kluczowe Wymagania i Warunki Realizacji**  1. Wykonawca jest zobowiązany do prowadzenia prac w taki sposób, aby zapewnić personelowi Zamawiającego transfer wiedzy umożliwiający samodzielne utrzymanie i doskonalenie SZBI po zakończeniu umowy. 2. Zamawiający zobowiązuje się do aktywnej współpracy z Wykonawcą, w tym do zapewnienia dostępu do niezbędnej dokumentacji, personelu oraz pomieszczeń w uzgodnionych terminach. 3. Wykonawca zobowiązany jest do realizacji zamówienia zgodnie z zasadą "nie czyń poważnych szkód" (DNSH - Do No Significant Harm), co oznacza, że wdrożone rozwiązania nie mogą wywierać negatywnego wpływu na cele środowiskowe. 4. Odbiór każdego etapu będzie następował na podstawie protokołu zdawczo-odbiorczego, podpisanego bez uwag przez obie strony, po weryfikacji kompletności i jakości dostarczonych produktów (deliverables). Zamawiający ma 10 dni roboczych na zgłoszenie uwag do przekazanych materiałów. 5. Wszystkie produkty cyfrowe (w tym m.in. raporty, polityki, procedury, materiały szkoleniowe) wytworzone przez Wykonawcę w ramach realizacji zamówienia muszą spełniać standardy dostępności cyfrowej określone w dokumencie "Standardy dostępności dla polityki spójności 2021-2027", co jest równoznaczne ze spełnieniem wymagań ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych i zgodnością z wytycznymi Web Content Accessibility Guidelines (WCAG) 2.1 na poziomie AA |

### Szkolenia dla kadry kierowniczej z zakresu SZBI

|  |
| --- |
| **1. Cel i Kontekst Zamówienia**  1.1. Cel główny:  Celem zamówienia jest wyposażenie kadry kierowniczej Zamawiającego w wiedzę i kompetencje niezbędne do świadomego zarządzania ryzykiem w obszarze cyberbezpieczeństwa, rozumienia kluczowej roli i odpowiedzialności menedżerów w Systemie Zarządzania Bezpieczeństwem Informacji (SZBI) oraz podejmowania strategicznych decyzji chroniących dane pacjentów, ciągłość działania placówki oraz jej reputację.  1.2. Grupa docelowa:  Szkolenie jest przeznaczone dla kadry kierowniczej Szpitala, w tym m.in. Dyrekcji, Ordynatorów, Kierowników oddziałów i działów administracyjnych. Szacowana liczba uczestników: do 50 osób.  **2. Szczegółowy Zakres Przedmiotu Zamówienia**  Przedmiotem zamówienia jest kompleksowa organizacja i przeprowadzenie jednego, jednodniowego szkolenia stacjonarnego w formie warsztatu w siedzibie Zamawiającego.  2.1. Minimalny zakres merytoryczny szkolenia:  Wykonawca jest zobowiązany zrealizować szkolenie obejmujące co najmniej następujące moduły tematyczne:   1. Zakres przedmiotowy i podmiotowy obowiązywania przepisów dotyczących cyberbezpieczeństwa. 2. Obowiązki podmiotów publicznych, w tym jednostek ochrony zdrowia. 3. Obowiązki podmiotu publicznego medycznego uznanego za operatora usługi kluczowej. 4. Struktura krajowego systemu cyberbezpieczeństwa. 5. Zadania i rola CSIRT NASK - Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego. 6. Wymagania prawne oraz znaczenie Systemu Zarządzania Bezpieczeństwem Informacji w organizacji. 7. Definicje i przykłady incydentów cyberbezpieczeństwa 8. Obsługa incydentów cyberbezpieczeństwa. 9. Wymagania dyrektywy NIS2 w obszarze cyberbezpieczeństwa i jej implementacja. 10. Rodzaje ataków **omówienie, przykłady oraz konsekwencje**:  * ataki socjotechniczne (phishing i jego rodzaje, Watering Hole, Baiting, Scareware, Deepfake ); * ataki na systemy i sieci (DDoS, Brute Force Attack, ataki na aplikacje webowe, ataki na urządzenia IoT, inżynieria wsteczna); * ataki Ransomware; * ataki na tożsamość; * wirusy – metodyka działania i metody ochrony.  1. AI - krótkie wprowadzenie do sztucznej inteligencji i przykłady jak może być wykorzystywana przeciwko nam. 2. HTTPS – dlaczego nie http. 3. WPA2 – dlaczego już nie jest bezpieczne. 4. Cała prawda o VPNach - czym są, co zapewniają a czego nie. 5. Kody QR. 6. MitM - nie tylko WiFi można podsłuchiwać 7. Zabezpieczenie informatycznych nośników danych – pendrivy i pamięci zewnętrzne. 8. Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia. 9. Przechowywanie  danych  w  chmurze  i  korzystanie  z  zewnętrznych  dostawców  usług informatycznych. 10. Prawidłowe korzystanie z oprogramowania antywirusowego. 11. Zasady aktualizacji programów i aplikacji. 12. Szyfrowanie dokumentów i poczty elektronicznej. 13. Polityka haseł, zarządzanie dostępem i tożsamością.   **2.2. Wymagania organizacyjne:**   * **Forma:** Szkolenie musi być przeprowadzone w formie interaktywnego warsztatu stacjonarnego. * **Lokalizacja:** Siedziba Zamawiającego. Zamawiający zapewni salę szkoleniową wyposażoną w rzutnik multimedialny. * **Czas trwania:** Minimum 5 godzin zegarowych (nie wliczając przerw). * **Termin realizacji:** Do uzgodnienia z Wykonawcą, jednak nie później niż do 60 dni od daty podpisania umowy. * **Materiały szkoleniowe:** Wykonawca jest zobowiązany przygotować i dostarczyć wszystkim uczestnikom materiały szkoleniowe w formie elektronicznej. * **Certyfikaty:** Wykonawca zapewni imienne certyfikaty ukończenia szkolenia dla wszystkich uczestników.   2.3. Wymagania wobec personelu Wykonawcy (Trenera):  Wykonawca musi zapewnić, że szkolenie zostanie przeprowadzone przez eksperta posiadającego:   * Minimum 3-letnie, udokumentowane doświadczenie zawodowe w obszarze cyberbezpieczeństwa i/lub wdrażania Systemów Zarządzania Bezpieczeństwem Informacji. * Udokumentowane doświadczenie w prowadzeniu szkoleń dla kadry kierowniczej.   **3. Warunki Realizacji i Odbioru Zamówienia**  **3.1. Odbiór prac:** Odbiór przedmiotu zamówienia nastąpi po zrealizowaniu szkolenia, na podstawie protokołu zdawczo-odbiorczego podpisanego bez uwag przez obie strony. Warunkiem podpisania protokołu jest dostarczenie przez Wykonawcę:   * Listy obecności uczestników szkolenia. * Materiałów szkoleniowych w wersji elektronicznej.   **3.2. Dostępność Cyfrowa:** Materiały szkoleniowe w wersji elektronicznej muszą spełniać standardy dostępności cyfrowej zgodne z wytycznymi WCAG 2.1 na poziomie AA. |

### Szkolenia dla personelu medycznego i administracyjnego z SZBI

|  |
| --- |
| Celem zamówienia jest podniesienie świadomości i kluczowych kompetencji personelu medycznego i administracyjnego Zamawiającego w zakresie fundamentalnych zasad cyberbezpieczeństwa oraz wewnętrznych regulacji dotyczących bezpieczeństwa informacji. Realizacja zamówienia ma na celu wzmocnienie odporności organizacji na incydenty bezpieczeństwa poprzez edukację pracowników.  **Grupa docelowa:** Szkolenie przeznaczone jest dla pracowników Zamawiającego, w tym personelu medycznego i administracyjnego.  **Szczegółowy Zakres Prac**  Przedmiot zamówienia obejmuje kompleksowe świadczenie usługi szkoleniowej w formie e-learningu, na które składają się dwa główne zadania:  **Zadanie 1: Dostarczenie i Utrzymanie Platformy E-learningowej**   1. **Dostęp:** Wykonawca zapewni dostęp do platformy szkoleniowej online dla **700 unikalnych użytkowników**. Dostęp do platformy musi być gwarantowany przez okres **minimum 12 miesięcy** od daty protokolarnego odbioru przedmiotu zamówienia. 2. **Wymagania Techniczne Platformy:**    * **Dostępność:** Platforma musi być dostępna dla użytkowników 24 godziny na dobę, 7 dni w tygodniu (gwarantowana dostępność na poziomie 99,5% w skali miesiąca).    * **Kompatybilność:** Platforma musi poprawnie funkcjonować na najnowszych, stabilnych wersjach popularnych przeglądarek internetowych: Google Chrome, Apple Safari, Microsoft Edge, na systemach operacyjnych Windows oraz macOS.    * **Zarządzanie Użytkownikami:** System musi umożliwiać rejestrację uczestników na podstawie adresów e-mail pochodzących z domen wskazanych przez Zamawiającego oraz na podstawie linku aktywacyjnego lub innego narzędzia pozwalajacego na rejestrację bez adresu e-mail. Zamawiający przekaże Wykonawcy listę domen uprawnionych do rejestracji. 3. **Wymagania Funkcjonalne Platformy:**    * **Automatyzacja i Monitoring:** Platforma musi zapewniać:      + Możliwość wysyłania automatycznych przypomnień e-mail do uczestników,      + Automatyczne generowanie imiennych certyfikatów ukończenia szkolenia (w formacie PDF) z możliwością ich samodzielnego pobrania przez uczestnika.   **Zadanie 2: Opracowanie i Udostępnienie Dedykowanych Kursów Szkoleniowych**  Na platformie, o której mowa w Zadaniu 1, Wykonawca udostępni kurs e-learningowy, którego treść zostanie opracowana w uzgodnieniu z Zamawiającym. Minimalny zakres merytoryczny kursu musi obejmować następujące moduły:   1. Obowiązki podmiotów publicznych, w tym jednostek ochrony zdrowia. 2. Obowiązki podmiotu publicznego medycznego uznanego za operatora usługi kluczowej. 3. Zadania i rola CSIRT NASK - Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego. 4. Definicje i przykłady incydentów cyberbezpieczeństwa 5. Obsługa incydentów cyberbezpieczeństwa. 6. Wymagania dyrektywy NIS2 w obszarze cyberbezpieczeństwa i jej implementacja. 7. Rodzaje ataków **omówienie, przykłady oraz konsekwencje**:  * ataki socjotechniczne (phishing i jego rodzaje, Watering Hole, Baiting, Scareware, Deepfake ); * ataki na systemy i sieci (DDoS, Brute Force Attack, ataki na aplikacje webowe, ataki na urządzenia IoT, inżynieria wsteczna); * ataki Ransomware; * ataki na tożsamość; * wirusy – metodyka działania i metody ochrony  1. AI - krótkie wprowadzenie do sztucznej inteligencji i przykłady jak może być wykorzystywana przeciwko nam. 2. HTTPS – dlaczego nie http 3. WPA2 – dlaczego już nie jest bezpieczne 4. Cała prawda o VPNach - czym są, co zapewniają a czego nie. 5. Kody QR. 6. MitM - nie tylko WiFi można podsłuchiwać 7. Zabezpieczenie informatycznych nośników danych – pendrivy i pamięci zewnętrzne. 8. Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia. 9. Przechowywanie  danych  w  chmurze  i  korzystanie  z  zewnętrznych  dostawców  usług informatycznych. 10. Prawidłowe korzystanie z oprogramowania antywirusowego. 11. Zasady aktualizacji programów i aplikacji. 12. Szyfrowanie dokumentów i poczty elektronicznej. 13. Polityka haseł, zarządzanie dostępem i tożsamością.   **Kluczowe Wymagania i Warunki Realizacji**   1. **Odbiór prac:** Odbiór przedmiotu zamówienia nastąpi na podstawie protokołu zdawczo-odbiorczego, podpisanego bez uwag przez obie strony, po weryfikacji przez Zamawiającego, że platforma e-learningowa została uruchomiona, jest w pełni funkcjonalna, zawiera kursy o wymaganym zakresie merytorycznym. 2. **Współpraca:** Zamawiający zobowiązuje się do aktywnej współpracy z Wykonawcą, w szczególności do przekazania listy domen e-mail uprawnionych do rejestracji na platformie. 3. **Dostępność Cyfrowa:** Interfejs platformy e-learningowej oraz wszystkie treści i produkty cyfrowe (materiały szkoleniowe, certyfikaty) wytworzone przez Wykonawcę muszą spełniać standardy dostępności cyfrowej określone w dokumencie "Standardy dostępności dla polityki spójności 2021-2027", co jest równoznaczne ze spełnieniem wymagań ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych i zgodnością z wytycznymi Web Content Accessibility Guidelines (WCAG) 2.1 na poziomie AA. 4. **Zasada DNSH:** Wykonawca zobowiązany jest do realizacji zamówienia zgodnie z zasadą "nie czyń poważnych szkód" (DNSH - Do No Significant Harm). 5. **Produkty/Deliverables (Przedmiot Odbioru):**  * Protokół potwierdzający udzielenie dostępu do w pełni funkcjonalnej platformy e-learningowej dla wskazanej liczby użytkowników na okres 12 miesięcy. |