Załącznik nr 1

do Zaproszenia

do składania ofert

**FORMULARZ OFERTY**

**na realizację projektu grantowego ze środków Krajowego Planu Odbudowy w ramach inwestycji D1.1.2. Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia (nabór konkurencyjny) pn. „CYFROWA TRANSFORMACJA POWIATOWEGO CENTRUM ZDROWIA   
W BRZEZINACH POPRZEZ WDROŻENIE E-USŁUG, DIGITALIZACJĘ DOKUMENTACJI I WZMOCNIENIE CYBERBEZPIECZEŃSTWA”, w zakresie wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnego   
z normą ISO/IEC 27001:2022, oraz w zakresie przygotowania i realizacji cyklu szkoleń z zakresu cyberbezpieczeństwa dla pracowników.**

1. **Oferent**

Nazwa: ………………………………………………………………………………………

……………………………………………………………………………………………….……………………………………………………………………………………………….

Adres: ……………………………………………………………………………………….

……………………………………………………………………………………………….……………………………………………………………………………………………….

NIP: ……………………………………………………………………………...………….

REGON: …………………………………………………………………………………….

Osoba do kontaktu (*imię, nazwisko, stanowisko, nr telefonu, adres e-mail*):

……………………………………………………………………………………………….

……………………………………………………………………………………………….

1. **Kryterium dostępu – doświadczenie Oferenta**

Proszę wypełnić tabelę:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Realizowane zadanie/ rodzaj doświadczenia** | **Zakres prac** | **Wartość brutto wykonanych prac** | **Termin wykonanych prac** | **Uwagi/ referencje** |
| 1. |  |  |  |  |  |
| 2. |  |  |  |  |  |
| 3. |  |  |  |  |  |

**Uwaga:** Tabelę można modyfikować wg potrzeb.

1. **Wartość oferty**

Proszę wypełnić tabelę. Przedmiot zamówienia obejmuje:

PAKIET A - wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnego z normą ISO/IEC 27001:2022

PAKIET B - przygotowanie i realizację cyklu szkoleń z zakresu cyberbezpieczeństwa dla pracowników PCZ w Brzezinach (kadra kierownicza – 36 osób, personel medyczny – 553 osoby, personel niemedyczny – 168 osób).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Przedmiot zamówienia** | **Cena jednostkowa netto (zł)** | **Wartość jednostkowa podatku VAT (zł)** | **Wartość brutto (zł)** |
| 1. | PAKIET A |  |  |  |
| 2 | PAKIET B |  |  |  |

**Uwaga:** Tabelę można modyfikować wg potrzeb.

1. **Potwierdzenie spełnienia wymagań.**

**PAKIET A - Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).**

|  |  |
| --- | --- |
| **Wymaganie** | **Spełnienie wymagania TAK/NIE/ dokumenty potwierdzające** |
| **1. Analiza wstępna oraz identyfikacja procesów organizacyjnych.** Wykonawca zobowiązuje się do przeprowadzenia kompleksowej analizy organizacji Zamawiającego w celu identyfikacji procesów wymagających objęcia Systemem Zarządzania Bezpieczeństwem Informacji (SZBI). Zakres prac obejmuje w szczególności: 1.1. Mapowanie procesów – identyfikacja procesów kluczowych i wspierających, ich właścicieli oraz zależności pomiędzy nimi. 1.2. Ocena dojrzałości obecnych praktyk bezpieczeństwa – weryfikacja stosowanych mechanizmów, norm, regulaminów i rozwiązań technicznych. 1.3. Identyfikacja luk w kontekście wymagań ISO 27001:2022 – w tym zestawienie aktualnych praktyk z wymaganiami normy oraz Załącznikiem A. 1.4. Przygotowanie dokumentu: „Lista zidentyfikowanych procesów organizacji wraz z oceną ich zgodności z ISO 27001:2022”. Produkt: • Raport z analizy wstępnej, w tym mapa procesów i ocena dojrzałości bezpieczeństwa. |  |
| **2. Inwentaryzacja aktywów informacyjnych i ocena ryzyka** Wykonawca przeprowadzi pełną identyfikację aktywów informacyjnych PCZ oraz analizę ryzyka zgodną z metodologią wymaganą normą ISO 27001:2022. Zakres prac obejmuje: 2.1. Identyfikacja aktywów informacyjnych – dane, systemy IT, zasoby ludzkie, środowisko fizyczne, sprzęt, usługi zewnętrzne, oprogramowanie, infrastruktura sieciowa. 2.2. Określenie właścicieli aktywów oraz relacji między aktywami. 2.3. Katalog zagrożeń i podatności – zgodnie z branżowymi standardami i Załącznikiem A. 2.4. Analiza ryzyka – ocena prawdopodobieństwa i wpływu incydentów bezpieczeństwa. 2.5. Opracowanie rejestru ryzyka oraz planu postępowania z ryzykiem – wskazanie sposobów redukcji, transferu, akceptacji lub unikania ryzyka. 2.6. Przygotowanie „Rejestru aktywów informacyjnych PCZ” w wersji sformalizowanej. Produkty: • Rejestr aktywów • Rejestr ryzyka • Plan postępowania z ryzykiem • Raport z przeprowadzonej analizy ryzyka |  |
| **3. Audyt zabezpieczeń w kontekście Załącznika A ISO 27001:2022** Wykonawca przeprowadzi audyt istniejących zabezpieczeń technicznych, fizycznych i organizacyjnych. Zakres prac obejmuje: 3.1. Weryfikacja zgodności z 93 kontrolami normy ISO 27001:2022 (kategorie: organizacyjne, ludzkie, fizyczne, technologiczne). 3.2. Ocena implementacji polityk i procedur, w tym zasad zarządzania dostępem, backupu, utrzymania infrastruktury IT, rozwoju systemów, nadzoru nad usługami zewnętrznymi. 3.3. Przegląd środowiska teleinformatycznego – zabezpieczenia sieci, serwerów, stacji roboczych, aplikacji oraz chmury. 3.4. Opracowanie katalogu luk oraz rekomendacji zmian. Produkt: • Raport z audytu zgodności z Załącznikiem A wraz z rekomendacjami wdrożenia. |  |
| **4. Opracowanie rekomendacji zabezpieczeń** Na podstawie wykonanej analizy ryzyka i audytu, Wykonawca opracuje zestaw rekomendowanych zabezpieczeń. Zakres prac obejmuje: 4.1. Dobór środków bezpieczeństwa zgodnie z wynikami analizy ryzyka oraz wymaganiami ISO 27001:2022. 4.2. Określenie priorytetów wdrożenia – plan działań krótko-, średnio- i długoterminowych. 4.3. Wycena ryzyk rezydualnych i ich akceptowalność. 4.4. Wsparcie w opracowaniu Deklaracji Stosowania (SoA). Produkt: • Deklaracja Stosowania (SoA) • Dokument „Rekomendacje zabezpieczeń wraz z mapą wdrożenia”. |  |
| **5. Opracowanie pełnej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji** Wykonawca przygotuje kompletną dokumentację SZBI w języku polskim, w tym: 5.1. Dokumenty obowiązkowe zgodnie z ISO 27001:2022, m.in.: • Zakres SZBI • Polityka Bezpieczeństwa Informacji • Cele bezpieczeństwa informacji • Rejestr ryzyka • Plan postępowania z ryzykiem • Deklaracja Stosowania • Rejestr aktywów • Polityka akceptowalnego użytkowania • Procedura zarządzania incydentami • Procedura ciągłości działania (BCP) lub integracja z istniejącą • Polityka haseł, dostępu, backupu, szyfrowania • Procedury operacyjne IT wraz z rozdziałem obowiązków • Polityka bezpieczeństwa dostawców i partnerów (w tym wzór klauzul umownych) • Zasady bezpiecznego rozwoju i utrzymania systemów IT • Polityka szkoleń i świadomości bezpieczeństwa • Procedura audytów wewnętrznych • Procedura nadzoru nad dokumentacją i zapisami • Raporty niezgodności i działań korygujących 5.2. Instrukcje robocze i formularze, w tym: • Wnioski o dostęp • Raport incydentu • Karta aktywa • Rejestr uprawnień • Wzory oświadczeń pracowniczych 5.3. Przygotowanie dokumentacji w wersji edytowalnej i gotowej do wdrożenia. Produkty: • Pełny komplet dokumentacji SZBI • Formularze i instrukcje • Raporty z przeprowadzonych prac |  |

**PAKIET B - Szkolenia z zakresu cyberbezpieczeństwa dla pracowników.**

|  |  |
| --- | --- |
| **Wymaganie** | **Spełnienie wymagania TAK/NIE/ dokumenty potwierdzające** |
| **1. Wymagania ogólne** Wykonawca zobowiązuje się do przygotowania i realizacji cyklu szkoleń  z zakresu cyberbezpieczeństwa (cyberhigieny) dla pracowników Zamawiającego, obejmujących: • kadrę kierowniczą (36 osób), • pracowników administracyjnych (168 osób), • pracowników medycznych (553 osoby).  Szkolenia muszą być przygotowane w oparciu o aktualne dobre praktyki rynkowe, zalecenia krajowych instytucji odpowiedzialnych za cyberbezpieczeństwo (np. CERT Polska, NASK, CSIRT sektorowe), europejskie standardy oraz wyniki ewentualnych audytów bezpieczeństwa przeprowadzonych u Zamawiającego. Usługa obejmuje zapewnienie dostępu do szkoleń przez okres 36 miesięcy (3 lata), w tym bieżącą obsługę uczestników. |  |
| **2. Modele realizacji szkoleń** Wykonawca zapewni dwa modele szkoleniowe: 2.1. Szkolenie stacjonarne / zdalne na żywo (dla kadry kierowniczej) • 1 szkolenie rocznie (minimum), • prowadzone w lokalizacji wskazanej przez Zamawiającego lub w formie wideokonferencji, • z interakcją z trenerem, możliwością zadawania pytań i analizą przykładów. 2.2. Szkolenia e learning (dla pracowników administracji i medycznych) • dostęp do platformy szkoleniowej wykonawcy lub równoważnej, • nieprzerwany dostęp do kursu przez okres 3 lat, • obsługa uczestników, raportowanie postępów i wyników, • możliwość wielokrotnego podchodzenia do materiału i testów. |  |
| **3. Ramowy zakres merytoryczny szkoleń** 3.1. Wprowadzenie do cyberbezpieczeństwa • podstawowe pojęcia: informacja, bezpieczeństwo informacji, cyberbezpieczeństwo, • znaczenie cyberbezpieczeństwa w działalności organizacji, • rodzaje informacji przetwarzanych w jednostce zdrowia. 3.2. Ochrona informacji • informacje wewnętrzne i dane osobowe, • podstawy ochrony danych, • zasady bezpieczeństwa dotyczące pracy z dokumentacją oraz systemami IT, • omówienie obowiązujących w PCZ regulacji wewnętrznych. 3.3. Rodzaje zagrożeń i metody działania cyberprzestępców • powszechne typy ataków cyfrowych, • charakterystyka phishingu, ransomware, socjotechniki, • identyfikowanie podejrzanych zachowań, wiadomości, załączników i stron internetowych. 3.4. Przykłady cyberzagrożeń (studia przypadków) • przykłady incydentów związanych z: • fałszywymi przesyłkami kurierskimi, • podszywaniem się pod dostawców usług, • zagrożeniami bankowymi i finansowymi, • serwisami ogłoszeniowymi, • mediami społecznościowymi. *(Poziom szczegółowości oraz liczba przykładów – po stronie wykonawcy.)* 3.5. Zasady ochrony przed cyberzagrożeniami • dobre praktyki cyberhigieny, • weryfikacja nadawcy, treści, załączników i linków, • zasady aktualizacji systemów i oprogramowania, • znaczenie narzędzi antywirusowych, • rekomendacje techniczne i organizacyjne. 3.6. Zasady bezpiecznego korzystania z systemów IT w PCZ • praca z systemami medycznymi i administracyjnymi, • ochrona haseł i kont, • podstawy bezpieczeństwa urządzeń mobilnych, • postępowanie w przypadku incydentów. 3.7. Test końcowy / Egzamin • min. 10 pytań jednokrotnego wyboru, • ocena zrozumienia materiału, • generowanie certyfikatów lub potwierdzeń ukończenia. |  |
| **4. Zakres dodatkowy dla kadry kierowniczej** Szkolenie dla kadry kierowniczej obejmuje dodatkowo: • podstawy regulacji prawnych z obszaru cyberbezpieczeństwa (np. KSC, RODO), • typy zagrożeń i ich wpływ na organizację, • procesy i zasady reagowania na incydenty, • podstawy nadzoru nad bezpieczeństwem informacji, • zasady prowadzenia testów oraz analiz bezpieczeństwa, • rola kierownictwa w zapewnieniu ciągłości działania i bezpieczeństwa danych. |  |
| **5. Zakres dodatkowy dla pracowników administracji i medycznych** Szkolenie dla tej grupy obejmuje: • podstawowe zasady cyberhigieny i bezpiecznej pracy z systemami IT, • omówienie najczęstszych ataków i sposobów ich rozpoznawania, • praktyczne przykłady incydentów, • zasady zgłaszania incydentów i nieprawidłowości, • odpowiedzialność prawna związana z niewłaściwym przetwarzaniem danych lub naruszeniem zasad bezpieczeństwa. |  |
| **6. Wymogi dotyczące ciągłości usług przez 3 lata** Wykonawca zapewni: • nieprzerwaną dostępność platformy e-learningowej, • bieżącą obsługę użytkowników (helpdesk, reset haseł, dostęp do kont), • aktualizację materiałów szkoleniowych w trakcie 36 miesięcy, • raportowanie ukończeń szkoleń na żądanie Zamawiającego, • odświeżone szkolenia lub webinary, jeżeli zajdzie potrzeba aktualizacji w związku z pojawieniem się nowych zagrożeń lub zmian przepisów. |  |
| **7. Produkty końcowe** W ramach realizacji usługi Wykonawca dostarczy: • dostęp do szkoleń e-learning dla wszystkich wskazanych pracowników przez 3 lata, • zrealizowane szkolenia stacjonarne/zdalne dla kadry kierowniczej, • raporty uczestnictwa i ukończeń, • testy i certyfikaty, • materiały szkoleniowe w wersji elektronicznej. |  |
| **8.Wymagania wobec firmy szkoleniowej/ trenerów**  8.1. Wykonawca musi posiadać statusu akredytowanego podmiotu szkoleniowego  Wykonawca musi posiadać co najmniej jeden z poniższych statusów:  • wpis do Rejestru Instytucji Szkoleniowych (RIS) prowadzonego przez WUP,  • status Niepublicznego Ośrodka Doskonalenia Nauczycieli lub inny ośrodek akredytowany przez MEiN,  • certyfikację instytucji szkoleniowej zgodną z:   * ISO 9001 (zarządzanie jakością), * ISO 29993 / ISO 29990 (jakość usług edukacyjnych – jeśli posiada). |  |
| 8.2. Każdy trener prowadzący szkolenia musi posiadać potwierdzone kompetencje  w zakresie cyberbezpieczeństwa.  Wymagane jest posiadanie co najmniej jednego z certyfikatów branżowych, np.: CompTIA Security+, CEH, CISA, CISSP, ISO/IEC 27001 Lead Auditor / Lead Implementer, Audytor Wiodący ISO 22301 / 27701 (mile widziane). |  |
| 8.3. Każdy trener prowadzący szkolenie musi posiadać doświadczenie szkoleniowe  • minimum 2 lata doświadczenia w prowadzeniu szkoleń z cyberbezpieczeństwa,  • minimum 5 przeprowadzonych szkoleń w ostatnich 24 miesiącach,  • doświadczenie w szkoleniach dla sektora ochrony zdrowia |  |
| 8.4. Każdy trener prowadzący szkolenie musi posiadać wiedzę potwierdzoną praktyką  • minimum roczne doświadczenie w pracy w obszarze IT/cyberbezpieczeństwa,  • znajomość specyfiki: HIS, PACS, EDM, danych medycznych, RODO. |  |
| **9. Wymagania wobec platformy e-learningowej**  Aby spełnić KPO, platforma szkoleniowa musi:  • Być zgodna z WCAG 2.1 na poziomie AA.  • Zapewniać pełną dostępność przez 36 miesięcy.  • Zapewniać monitoring aktywności użytkowników (logi, postępy, raporty).  • Przechowywać dane zgodnie z RODO na terenie UE.  • Umożliwiać testy, certyfikaty oraz archiwizację wyników. |  |
| **10. Wymogi dotyczące materiałów szkoleniowych**  Materiały muszą:  • Zawierać odniesienia do: KSC, RODO, zaleceń NASK, CERT Polska, ENISA, zaleceń CSIRT sektorowych.  • Być aktualizowane w trakcie 36 miesięcy.  • Być zgodne z zasadami KPO: dostępne cyfrowo (PDF/HTML), zgodne z WCAG 2.1 AA. |  |
| **11.Wymagania dotyczące zgodności z KPO**  Wykonawca musi:  11.1. Spełniać zasady KPO, w tym:  • Zasadę DNSH (Do No Significant Harm) – oświadczenie Wykonawcy,  • Wymogi dotyczące cyfrowej odporności i bezpieczeństwa usług,  • Wymóg utrzymania rezultatów przez okres min. 5 lat (szkolenia i materiały muszą być dostępne). |  |
| 11.2. Prowadzić dokumentację zgodnie z wymogami KPO  • listy obecności,  • raporty postępów,  • certyfikaty niezależne,  • dokumenty potwierdzające dostępność cyfrową |  |
| 11.3. Zapewnić raportowanie postępów • raporty kwartalne,  • rejestry ukończonych szkoleń,  • statystyki aktywności uczestników. |  |

1. **Dane i podpis/y osoby/osób reprezentujących Oferenta (*imię i nazwisko, stanowisko, podpis*)**

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

1. **Informacja o przetwarzaniu danych osobowych (RODO)**

Podpisanie i złożenie oferty jest jednocześnie potwierdzeniem akceptacji projektu umowy stanowiącej załącznik nr 2 do zaproszenia do składania ofert oraz zgodą na przetwarzanie danych osobowych, zgodnie z obowiązującymi przepisami, zawartych w formularzu ofertowym dla potrzeb przeprowadzenia niniejszego postępowania.

Administratorem danych osobowych jest **Powiatowe Centrum Zdrowia sp. z o.o.  
w Brzezinach**, ul. M. Skłodowskiej-Curie 6, 95-060 Brzeziny.