

ZAPROSZENIE DO SKŁADANIA OFERT

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.

I. Zamawiający

Powiatowe Centrum Zdrowia sp. z o.o. zs. w Brzezinach (95-060) przy ul. M. Skłodowskiej – Curie 6, KRS: 0000314018, NIP: 833-138-44-12, REGON: 100576369

II. Adres inwestycji

ul. M. Skłodowskiej – Curie 6, 95-060 Brzeziny, Gmina Brzeziny, Powiat Brzeziński, województwo łódzkie

III. Cel inwestycji

Celem inwestycji jest zwiększenie poziomu bezpieczeństwa informacji w organizacji poprzez kompleksowe wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnego z normą ISO/IEC 27001:2022 obejmującego wszystkie etapy niezbędne do zaprojektowania, przygotowania i wdrożenia systemu w organizacji Zamawiającego oraz przygotowanie i realizację cyklu szkoleń z zakresu cyberbezpieczeństwa dla wszystkich grup pracowników, w tym kadry kierowniczej (36 osób), personelu medycznego (553 osoby) i personelu niemedycznego (168 osób), w celu podniesienia świadomości zagrożeń i zapewnienia bezpiecznego przetwarzania danych.

IV. Zakres rzeczowy postępowania

PAKIET A – Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

1. Analiza wstępna oraz identyfikacja procesów organizacyjnych.

Wykonawca przeprowadzi kompleksową analizę 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. Ocenę dojrzałości obecnych praktyk bezpieczeństwa – weryfikacja stosowanych mechanizmów, norm, regulaminów i rozwiązań technicznych.
- 1.3. Identyfikację 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”.

Rezultaty:

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 w Brzezinach oraz analizę ryzyka zgodną z metodologią wymaganą normą ISO 27001:2022. Zakres prac obejmuje w szczególności:

- 2.1. Identyfikację 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. Analizę 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.

Rezultaty:

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 w szczególności:

- 3.1. Weryfikację zgodności z 93 kontrolami normy ISO 27001:2022 (kategorie: organizacyjne, ludzkie, fizyczne, technologiczne).
- 3.2. Ocenę 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.

Rezultaty:

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 w szczególności:

- 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. Wycenę ryzyk rezydualnych i ich akceptowalność.
- 4.4. Wsparcie w opracowaniu Deklaracji Stosowania (SoA).

Rezultaty:

Deklaracja Stosowania (SoA), dokument „Rekomendacje zabezpieczeń wraz z mapą wdrożenia”.

5. Opracowanie pełnej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

Wykonawca przygotowuje kompletną dokumentację SZBI w języku polskim, obejmującą:

5.1. Dokumenty obowiązkowe zgodnie z ISO 27001:2022, w tym:

- 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. Dokumentację w wersji edytowalnej i gotowej do wdrożenia.

Rezultaty:

Pełen komplet dokumentacji SZBI, formularze i instrukcje, raporty z przeprowadzonych prac.

PAKIET B – Szkolenia z zakresu cyberbezpieczeństwa dla pracowników

1. Ogólny opis usługi szkoleniowej

Wykonawca zobowiązuje się do przygotowania i realizacji cyklu szkoleń z zakresu cyberbezpieczeństwa (cyberhigieny) dla pracowników Zamawiającego, obejmujących:

- kadre 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: **stacjonarne i e-learning**.

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 w Brzezinach.**

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 winno dodatkowo obejmować:

- 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 winno dodatkowo obejmować:

- 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.

Jeżeli w powyższym opisie przedmiotu zamówienia znajdują się wskazania znaków towarowych, patentów lub pochodzenia, należy przyjąć, że wskazaniu takiemu towarzyszą wyrazy „lub równoważny”. Dopuszcza się więc wszelkie równoważne odpowiedniki rynkowe o właściwościach nie gorszych niż wskazane. Parametry wskazanego standardu określają minimalne warunki techniczne, eksploatacyjne, użytkowe, jakościowe i funkcjonalne, jakie ma spełnić przedmiot zamówienia. Wskazane znaki towarowe, patenty, marki lub nazwy producenta wskazujące na pochodzenie określają jedynie klasę produktu, metody, materiałów, urządzeń, systemów, technologii itp. Można więc przyjąć metody, materiały, urządzenia, systemy, technologie itp. innych marek i producentów, jednak o parametrach technicznych, jakościowych i właściwościach użytkowych oraz funkcjonalnych odpowiadających metodom, materiałom, urządzeniom, systemom i technologiom itp. powyżej opisanym. Dodatkowo Zamawiający podkreśla, że równoważne metody, materiały, urządzenia, systemy, technologie itp. nie mogą stanowić zamienników w stosunku do metod, materiałów, urządzeń, systemów, technologii itp. opisanych w dokumentacji za pomocą znaków towarowych, patentów, pochodzenia.

V. Termin realizacji zadania

Termin realizacji: 30.04.2026 r.

VI. Warunki i zabezpieczenie realizacji zadania

1. Termin i miejsce realizacji usługi muszą być uzgodnione z Project Manager ds. projektów IT: tel. 603 331 471, e-mail: h.pachowski@szpital-brzeziny.pl.
2. Dostarczona wraz z usługą dokumentacja musi być sporządzona w języku polskim.
3. Realizacja usługi musi zostać potwierdzona protokołem.
4. Wykonawca zobowiązany jest do zapewnienia zespołu projektowego oraz wyznaczenia kierownika projektu posiadającego doświadczenie w realizacji projektów odpowiadających zakresowi PAKIETÓW.
5. Zamawiający wymaga, aby Oferent posiadał aktualne **ubezpieczenie OC** na okres realizacji zadania w zakresie prowadzonej działalności gospodarczej, związanej z przedmiotem zamówienia, na kwotę gwarancyjną nie mniejszą niż kwota 70 000,00 zł w ramach **PAKIETU A** oraz nie mniejszą niż 30 000,00 zł w ramach **PAKIETU B**.

Potwierdzenie ubezpieczenia stanowić będzie załącznik do umowy.

6. Zamawiający wymaga wykazania przez Oferenta:

- a) w ramach **PAKIETU A** – doświadczenia w realizacji co najmniej 5 wdrożeń SZBI zgodnych z normą ISO/IEC 27001, zrealizowanych w latach 2023–2025;
- b) w ramach **PAKIETU B** – doświadczenia w prowadzeniu szkoleń z zakresu cyberbezpieczeństwa, potwierdzonego wykazem szkoleń zrealizowanych w okresie ostatnich 3 lat oraz referencjami z realizacji szkoleń dla co najmniej dwóch różnych instytucji publicznych.

Warunek ten stanowi kryterium dostępu w postępowaniu, co oznacza, że Zamawiający będzie rozpatrywał tylko oferty oferentów spełniających ten warunek.

VII. Etapy wyboru wykonawcy zadania

I etap – od 30.01.2026 r. do 02.03.2026 r. do godziny 23:59

Złożenie podpisanej oferty.

Do dnia 15.02.2026 r. do godziny 23:59 Oferenci mogą zadawać pytania, na które Zamawiający odpowie w terminie do dnia 20.02.2026 r.

II etap – od 03.03.2026 r. do 04.03.2026 r.

Ocena złożonych ofert w zakresie opisanym kryteriami oceny ofert. W przypadku wątpliwości dotyczących oceny oferty, Oferent może zostać wezwany do złożenia dodatkowych wyjaśnień i informacji.

Zamawiający ma prawo do odrzucenia ofert z rażąco niską ceną lub rażąco wysoką ceną.

III etap – 05.03.2026 r. do 06.03.2026 r.

Wybór Wykonawcy. Podpisanie umowy.

VIII. Kryteria oceny ofert

Cena – 100%

W kryterium „Cena” oferta otrzyma zaokrągloną do dwóch miejsc po przecinku liczbę punktów wynikająca z następującego działania:

$W_{kc} = (C_{min} / C_{of}) \times 100 \times W_k$, gdzie: W_{kc} – wartość kryterium „Cena”

W_{kc} – wartość kryterium „Cena”

C_{min} – najniższa cena brutto zaoferowana w postępowaniu

C_{of} – cena brutto zaproponowana przez Oferenta

W_k – waga kryterium (100%)

IX. Sposób przygotowania oferty

Ofertę należy przygotować poprzez szczegółowe wypełnienie i podpisanie formularza oferty wraz z oświadczeniem stanowiącym załącznik nr 3 do zaproszenia.

X. Termin składania ofert

Oferty należy złożyć w terminie do **02.03.2026 r.**

Złożenie oferty jest jednoznaczne z akceptacją projektu umowy, stanowiącego załącznik do Zaproszenia do składania ofert.

XI. Osoby do kontaktu

Hubert Pachowski - Project Manager ds. projektów IT

tel. 603 331 471, e-mail: h.pachowski@szpital-brzeziny.pl

Aneta Kurzyńska – Dyrektor ds. Infrastruktury i Inwestycji,

tel. 500 044 688, e-mail: a.kurzynska@szpital-brzeziny.pl

Marta Matachowska – Inspektor ds. administracji i zamówień,

tel. 723 288 701, e-mail: m.matachowska@szpital-brzeziny.pl

XII. Postanowienia końcowe

1. Zgodnie z dyspozycją art. 4c ustawy z dnia 8 marca 2013 roku o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (Dz. U. z 2019 r. poz. 118 z późn. zm.) **Powiatowe Centrum Zdrowia z w Brzezinach Sp. o.o.** oświadcza, że posiada status dużego przedsiębiorcy w rozumieniu przepisów tej ustawy.
2. Zamawiający ma prawo do unieważnienia postępowania bez podawania przyczyny. Unieważnienie postępowania nie generuje roszczeń po stronie Oferentów.

XIII. Załączniki

1. Formularz oferty
2. Projekt umowy
3. Oświadczenie o braku powiązań kapitałowych z Zamawiającym