**Przeprowadzenie diagnozy cyberbezpieczeństwa oraz szkoleń w zakresie cyberbezpieczeństwa**

1. **Opis przedmiotu zamówienia.**
	1. Przedmiotem zamówienia jest przeprowadzeniu **diagnozy cyberbezpieczeństwa, audytu KRI, testów penetracyjnych, dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz szkoleń** w zakresie cyberbezpieczeństwa w ramach realizacji projektu realizowanego w ramach umowy o powierzenie grantu o numerze 4676/3/2022 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020, Oś V. Rozwój cyfrowy 1ST oraz. wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU. Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia zwanego dalej ..Projektem".
	2. Diagnoza musi być przeprowadzona przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu,
	3. Szczegółowy Opis Przedmiotu Zamówienia stanowi Załącznik nr 1 do OPZ.
	4. Oznaczenie przedmiotu zamówienia wg. Wspólnego Słownika Zamówień (CPV): usługi audytu 79212000-3; szkolenia - usługi szkoleniowe 80500000-9.
2. **Termin wykonania zamówienia.**
	1. Termin realizacji zamówienia:

Przeprowadzenie diagnozy cyberbezpieczeństwa – do dnia 15.10.2022 r.

Pozostały zakres – 4 miesiące od daty podpisania umowy

* 1. Za datę zawarcia umowy Zamawiający przyjmuje dzień, w którym zostanie ona podpisana przez obie Strony umowy.
1. **Warunki udziału w postępowaniu.**

5.1. Doświadczenie Wykonawcy:

# Warunki równoważności

Wszędzie gdzie użyto nazw własnych produktów oraz nazwy certyfikatów Zamawiający stosuje zasadę równoważności która określa przedmiot zamówienia o cechach technicznych, jakościowych lub funkcjonalnych takich samych lub zbliżonych do tych, które zawiera zakres równoważności wskazany w opisie przedmiotu zamówienia, lecz oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.

W przypadku wątpliwości Zamawiający oczekuje pytań ze strony Wykonawcy, które będą zawierały odniesienie do rozwiązania lub certyfikatu uważanego za równoważny przez Wykonawcę z oczekiwanym przez Zamawiającego.

Zamawiający dopuści rozwiązania równoważne o ile zagwarantują one takie same parametry jakościowe dla zaoferowanych usług jak oczekiwane przez Zamawiającego.

# Wymagania wobec Wykonawcy

Wykonawca musi posiadać wiedzę i doświadczenie poparte odpowiednimi referencjami w zakresie audytu bezpieczeństwa oraz dołączyć:

Wykonawca w ciągu ostatnich trzech lat, a jeżeli okres prowadzenia działalności jest krótszy wykonał, na potwierdzenie którego powinien przedstawić:

* co najmniej pięć referencji, protokołów odbioru lub umów poświadczających przeprowadzenie audytu bezpieczeństwa w jednostkach administracji publicznej z należytą starannością w zakresie spełnienia wymagań wynikających ISO 27001 albo KRI o wartości brutto 4000,00 każdy,
* co najmniej pięć referencji, protokołów odbioru lub umów poświadczających przeprowadzenie audytu bezpieczeństwa w jednostkach administracji publicznej z należytą starannością w zakresie wynikającym projektu Cyfrowa Gmina,
* co najmniej trzy referencje, protokoły odbioru lub umowy poświadczające przeprowadzenie testów penetracyjnych aplikacji webowych w jednostkach administracji publicznej z należytą starannością o wartości 20 000,00 zł brutto każda,
* co najmniej jedna referencja, protokół odbioru lub umowa poświadczająca przeprowadzenie testów socjotechnicznych w sektorze publicznym albo w podmiotach prowadzących działalność komercyjną z należytą starannością o wartości 17 000,00 brutto
* co najmniej 10 szkoleń, których przedmiotem było bezpieczeństwo informacji oraz ochrona danych osobowych w jednostkach sektora publicznego,
* co najmniej 5 referencji, protokołów odbioru lub umów poświadczających wykonanie wdrożenia systemu bezpiecznej poczty elektronicznej w chmurze

# Wymagania wobec osób realizujących przedmiot zamówienia

* osobami posiadającymi wiedzę i doświadczenie zgodnie z zakresem opisanym poniżej:
	+ Tester bezpieczeństwa – przynajmniej jedna osoba musi posiadać:
		- co najmniej 3 letnie doświadczenie w zakresie pełnienia funkcji testera bezpieczeństwa (pentestera) \*,
		- certyfikat OSCP (Offensive Security Certified Professional),
		- certyfikat uprawniający do przeprowadzenia audytu zgodnie z rozporządzeniem

Ministra Cyfryzacji 1 z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu,

* + - co najmniej 3 letnie doświadczenie w zakresie prowadzenia audytów bezpieczeństwa uwzględniających założenia wynikające z normy ISO 27001,
	+ Audytor bezpieczeństwa – przynajmniej jedna osoba musi posiadać:
		- co najmniej 3 letnie doświadczenie w zakresie prowadzenia audytów bezpieczeństwa uwzględniających założenia wynikające z normy ISO 27001 i/lub KRI,
		- certyfikat uprawniający do przeprowadzenia audytu zgodnie z rozporządzeniem

Ministra Cyfryzacji 1 z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu,

* + - doświadczenie w prowadzeniu szkoleń w zakresie cyberbezpieczeństwa, którego tematyką była co najmniej ochrona przed złośliwym oprogramowaniem, socjotechniką w tym phishingiem, bezpiecznym korzystaniem z poczty elektronicznej oraz Internetu, wykorzystaniem menadżera haseł,
	+ Tester bezpieczeństwa (socjotechnika) – przynajmniej jedna osoba musi posiadać:
		- co najmniej 3 letnie doświadczenie w zakresie pełnienia funkcji testera bezpieczeństwa (pentestera) \*,
		- certyfikat OSCP (Offensive Security Certified Professional),
		- posiadać wiedzę i doświadczenie w zakresie przygotowywania oraz wykonywania testów socjotechnicznych,
	+ Audytor bezpieczeństwa (dokumentalista) – przynajmniej jedna osoba musi posiadać:
		- co najmniej 3 letnie doświadczenie w zakresie prowadzenia audytów bezpieczeństwa uwzględniających założenia wynikające z normy ISO 27001 i/lub KRI,
		- certyfikat uprawniający do przeprowadzenia audytu zgodnie z rozporządzeniem
		- Ministra Cyfryzacji 1 z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu,
		- doświadczenie w przygotowaniu kompleksowej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z normą ISO 27001:2017 poparte jedną referencją imienną albo protokołem odbioru zadania, w którym wskazana osoba brała udział i widnieje jej nazwisko albo innym dokumentem, poświadczonym przez Klienta, na podstawie którego możliwe jest stwierdzenie, że wybrana osoba realizowała przedmiot projektu,

\* - przez testy penetracyjne należy rozumieć przeprowadzenie testów mających na celu wykrycie nieznanych podatności. Skanowanie pod kątem znanych podatności narzędziami typu Nessus, OpenVAS (Greenbone), BurpSuite, Acunetix i inne podobne nie spełnia wymagania testów penetracyjnych.

Zamawiający nie dopuszcza łączenia kompetencji ani osób wskazanych do realizacji przedmiotu projektu . Wykonawca wskaże w ramach oferty osoby wraz z przypisaniem każdej z nich do pełnionej roli.

**Niepotwierdzenie powyższych wymagań skutkować będzie odrzuceniem oferty.**

1. **Informacja na temat zakresu wykluczenia z powodu powiązań osobowych lub kapitałowych.**
	1. W celu uniknięcia konfliktu interesów zamówienia publiczne, nie będą udzielane podmiotom powiązanym osobowo lub kapitałowo z Zamawiającym. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przeprowadzeniem procedury wyboru Wykonawcy a Wykonawcą, polegające w' szczególności na:
	2. uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej,
	3. posiadaniu, co najmniej 10 % udziałów lub akcji.
	4. pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika.
	5. pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.
	6. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. 2022 poz. 835).
	7. Stosowne oświadczenia Wykonawcy zamieszczono w załączniku nr 2 do SWZ.
2. **Kryteria oceny ofert.**
	1. Kryterium oceny ofert - Cena 100%
	2. Wykonawca określi cenę oferty, która stanowić będzie wynagrodzenie ryczałtowe za realizację całego przedmiotu zamówienia, podając ją w zapisie liczbowym i słownie z dokładnością do grosza (do dwóch miejsc po przecinku).
	3. Cena oferty musi zawierać wszystkie koszty niezbędne do zrealizowania przedmiotu zamówienia. Wykonawca musi uwzględnić w cenie oferty wszelkie koszty niezbędne dla prawidłowego i pełnego wykonania zamówienia ujęte w zał. nr 1 do Zapytania w tym koszty dojazdu, materiały szkoleniowe oraz wszelkie opłaty i podatki wynikające z obowiązujących przepisów.
	4. Za najkorzystniejszą zostanie uznana oferta Wykonawcy, który zaoferuje najniższą cenę całkowitą za wykonanie przedmiotu zamówienia.
3. **Sposób przy gotowania ofert i termin ich składania.**
	1. Wykonawca może złożyć tylko jedną ofertę na całość Zapytania ofertowego, **bez możliwości złożenia oferty częściowej.**
	2. Oferta musi być podpisana przez Wykonawcę, tj. osobę (osoby) reprezentującą Wykonawcę, zgodnie z zasadami reprezentacji wskazanymi we właściwym rejestrze lub osobę (osoby) upoważnioną do reprezentowania Wykonawcy. Jeżeli w imieniu Wykonawcy działa osoba, której umocowanie do jego reprezentowania nie wynika z właściwego rejestru, Zamawiający żąda od Wykonawcy pełnomocnictwa lub innego dokumentu potwierdzającego umocowanie do reprezentowania Wykonawcy.
	3. Oferta niepodpisana zostanie odrzucona.
	4. Jeżeli zostanie złożona oferta, której wybór będzie prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia i 1marca 2004 r. o podatku od towarów i usług, dla celów zastosowania kryterium ceny Zamawiający doliczy do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć. W takim przypadku Wykonawca ma obowiązek:
		1. poinformowania Zamawiającego, że wybór jego oferty będzie prowadził do powstania u

Zamawiającego obowiązku podatkowego;

* + 1. wskazania nazwy (rodzaju) towaru i/lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;
		2. wskazania wartości towaru i/łub usługi objętego obowiązkiem podatkowym

Zamawiającego, bez kwoty podatku;

* + 1. wskazania stawki podatku od towarów i/lub usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.
	1. W przypadku rozbieżności w Formularzu ofertowym pomiędzy kwotami netto, brutto lub słownie, Zamawiający poprawi stosując zasady arytmetyki przyjmując za punkt wyjścia cenę jednostkową netto wpisaną liczbowo w Formularzu ofertowym dla poszczególnych kosztów.
	2. Zamawiający nie przewiduje publicznego otwarcia ofert.
1. **Istotne postanowienia umowy.**
	1. Zamawiający zawrze umowę z Wykonawcą na warunkach określonych w projekcie umowy
	2. Postanowienia zawarte w projekcie umowy nie podlegają negocjacjom.
	3. Wykonawca akceptuje treść projektu umowy oświadczeniem zawartym w treści Formularza ofertowego.
2. **Informacje o formalnościach, jakie muszą zostać dopełnione przed zawarciem umowy.**
	1. Zamawiający poinformuje Wykonawcę, którego oferta została wybrana, jako najkorzystniejsza o miejscu i terminie zawarcia umowy.
	2. Niedopełnienie obowiązków wskazanych powyżej w terminie wyznaczonym przez Zamawiającego może zostać uznane przez Zamawiającego za równoznaczne z odmową lub uchylaniem się Wykonawcy od podpisania umowy.
3. **Wyjaśnienia oraz uzupełnienie oferty**
	1. W toku badania ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonej oferty, treści oświadczeń, dokumentów, pełnomocnictw i ich uzupełnienia.
	2. Jeżeli zaoferowana cena będzie rażąco niska w stosunku do przedmiotu zamówienia lub będzie budziła wątpliwości co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi przez Zamawiającego lub wynikającymi z odrębnych przepisów, Zamawiający zwróci się do Wykonawcy o udzielenie wyjaśnień, w tym złożenie dowodów dotyczących wyliczenia ceny. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny lub kosztu będzie spoczywać na Wykonawcy.
	3. Zamawiający odrzuci ofertę Wykonawcy, który nie udzieli wyjaśnień, o których mowa powyżej lub jeżeli dokonana ocena tych wyjaśnień wraz ze złożonymi dowodami potwierdzi, że zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia.
4. **Ewentualne Informacje o sposobie porozumiewania się**

Pracownikiem uprawnionym do kontaktowania się z Wykonawcami jest: Maciej Barycz - tel. 18 548 02 38, e-mail: informatyk@chelmiec.pl, Katarzyna Smoleń – tel. 18 548 02 24, e-mail: przetargi@chelmiec.pl

1. **Informacje końcowe.**
	1. Zamówienie jest współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa, Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU. Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia.