

**Ogłoszenie o zamówieniu
Usługi**

Zakup usług audytu bezpieczeństwa, testów penetracyjnych, testów socjotechnicznych, SZBI oraz szkoleń dedykowanych dla Urzędu Gminy Dobra i jedn. podległ. w ramach projektu Cyberbezpieczna Gmina Dobra

SEKCJA I - ZAMAWIAJĄCY

1.1.) Rola zamawiającego

Postępowanie prowadzone jest samodzielnie przez zamawiającego

1.2.) Nazwa zamawiającego: Gmina Dobra

1.3.) Oddział zamawiającego: Urząd Gminy Dobra

1.4) Krajowy Numer Identyfikacyjny: REGON 491892185

1.5) Adres zamawiającego

1.5.1.) Ulica: Dobra 233

1.5.2.) Miejscowość: Dobra

1.5.3.) Kod pocztowy: 34-642

1.5.4.) Województwo: małopolskie

1.5.5.) Kraj: Polska

1.5.6.) Lokalizacja NUTS 3: PL218 - Nowosądecki

1.5.7.) Numer telefonu: 183330020

1.5.9.) Adres poczty elektronicznej: sekretariat@gminadobra.pl

1.5.10.) Adres strony internetowej zamawiającego: www.gminadobra.pl

1.6.) Rodzaj zamawiającego: Zamawiający publiczny - jednostka sektora finansów publicznych - jednostka samorządu terytorialnego

1.7.) Przedmiot działalności zamawiającego: Ogólne usługi publiczne

SEKCJA II – INFORMACJE PODSTAWOWE

2.1.) Ogłoszenie dotyczy:

Zamówienia publicznego

2.2.) Ogłoszenie dotyczy usług społecznych i innych szczególnych usług: Nie

2.3.) Nazwa zamówienia albo umowy ramowej:

Zakup usług audytu bezpieczeństwa, testów penetracyjnych, testów socjotechnicznych, SZBI oraz szkoleń dedykowanych dla Urzędu Gminy Dobra i jedn. podległ. w ramach projektu Cyberbezpieczna Gmina Dobra

2.4.) Identyfikator postępowania: ocds-148610-d328cb10-9110-408d-8f8d-0f088f57af36

2.5.) Numer ogłoszenia: 2026/BZP 00385401

2.6.) Wersja ogłoszenia: 01

2.7.) Data ogłoszenia: 2026-08-10

2.8.) Zamówienie albo umowa ramowa zostały ujęte w planie postępowań: Nie

2.11.) O udzielenie zamówienia mogą ubiegać się wyłącznie wykonawcy, o których mowa w art. 94 ustawy: Nie

2.14.) Czy zamówienie albo umowa ramowa dotyczy projektu lub programu współfinansowanego ze środków Unii Europejskiej: Tak

2.15.) Nazwa projektu lub programu

Fundusze Europejskie na Rozwój Cyfrowy (FERC) Priorytet II Zaawansowane usługi cyfrowe Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa Fundusz Europejski Fundusz Rozwoju Regionalnego (EFRR) Numer naboru

FERC.02.02-CS.01-001/23.

2.16.) Tryb udzielenia zamówienia wraz z podstawą prawną

Zamówienie udzielane jest w trybie podstawowym na podstawie: art. 275 pkt 1 ustawy

SEKCJA III – UDOSTĘPNIANIE DOKUMENTÓW ZAMÓWIENIA I KOMUNIKACJA**3.1.) Adres strony internetowej prowadzonego postępowania**<https://ezamowienia.gov.pl/mp-client/search/list/ocds-148610-d328cb10-9110-408d-8f8d-0f088f57af36>**3.2.) Zamawiający zastrzega dostęp do dokumentów zamówienia: Nie****3.4.) Wykonawcy zobowiązani są do składania ofert, wniosków o dopuszczenie do udziału w postępowaniu, oświadczeń oraz innych dokumentów wyłącznie przy użyciu środków komunikacji elektronicznej: Tak**

3.5.) Informacje o środkach komunikacji elektronicznej, przy użyciu których zamawiający będzie komunikował się z wykonawcami - adres strony internetowej: Komunikacja między Zamawiającym a Wykonawcami odbywa się przy użyciu Platformy e-Zamówienia, która jest dostępna pod adresem: <https://ezamowienia.gov.pl>. Korzystanie z Platformy e-Zamówienia jest bezpłatne. W szczególnie uzasadnionych przypadkach uniemożliwiających komunikację Wykonawcy i Zamawiającego za pośrednictwem Platformy e-Zamówienia (np. awaria Platformy lub jej niedostępność), Zamawiający dopuszcza komunikację za pomocą poczty elektronicznej na adres: e-mail: sekretariat@gminadobra.pl (nie dotyczy składania ofert). Adres strony internetowej prowadzonego postępowania (link prowadzący bezpośrednio do widoku postępowania na Platformie e- Zamówienia) dostępny wyżej w ogłoszeniu. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego musi posiadać konto podmiotu „Wykonawca” na Platformie e-Zamówienia. Szczegółowe informacje na temat zakładania kont podmiotów oraz zasady i warunki korzystania z Platformy e-Zamówienia określa Regulamin Platformy.

3.6.) Wymagania techniczne i organizacyjne dotyczące korespondencji elektronicznej: Komunikacja w postępowaniu, z wyłączeniem składania ofert, odbywa się drogą elektroniczną za pośrednictwem formularzy do komunikacji dostępnych w zakładce „Formularze” („Formularze do komunikacji”). Za pośrednictwem „Formularzy do komunikacji” odbywa się w szczególności przekazywanie wezwań i zawiadomień, zadawanie pytań i udzielanie odpowiedzi. Formularze do komunikacji umożliwiają również dołączenie załącznika do przesyłanej wiadomości (przycisk „dodaj załącznik”). Możliwość korzystania w postępowaniu z „Formularzy do komunikacji” w pełnym zakresie wymaga posiadania konta „Wykonawcy” na Platformie e-Zamówienia oraz zalogowania się na Platformie e-Zamówienia. Maksymalny rozmiar plików przesyłanych za pośrednictwem „Formularzy do komunikacji” wynosi 150 MB (wielkość ta dotyczy plików przesyłanych jako załączniki do jednego formularza). Minimalne wymagania techniczne dotyczące sprzętu używanego w celu korzystania z usług Platformy e-Zamówienia oraz informacje dotyczące specyfikacji połączenia określa Regulamin Platformy e- Zamówienia. Zgodnie z § 12 ww. Regulaminu w celu prawidłowego korzystania z usług Platformy eZamówienia wymagany jest: Komputer PC, a. parametry minimum: Intel Core2 Duo, 2 GB RAM, HDD, b. zainstalowany jeden z następujących systemów operacyjnych: MS Windows 7 lub nowszy, OSX/Mac OS 10.10, Ubuntu 14.04, c. Zainstalowana jedna z następujących przeglądark: Chrome 66.0 lub nowsza, Firefox 59.0 lub nowszy, Safari 11.1 lub nowszaEdge 14.0 i nowsze albo Tablet/Telefon: a. parametry minimum: 4 rdzenie procesora, 2GB RAM, Android 6.0 Marshmallow, iOS 10.3, b. przeglądarka Chrome 61 lub nowsza. Dla skorzystania z pełnej funkcjonalności może być konieczne włączenie w przeglądarce obsługi protokołu bezpiecznej transmisji danych SSL, obsługi Java Script, oraz cookies; Specyfikacja połączenia, formatu przesyłanych danych oraz kodowania i oznaczania czasu odbioru danych: 1.1 specyfikacja połączenia – formularze udostępnione są za pomocą protokołu TLS 1.2, 1.2 format danych oraz kodowanie: formularze dostępne są w formacie HTML z kodowaniem UTF-8 1.3 oznaczenia czasu odbioru danych: wszelkie operacje opierają się o czas serwera i dane zapisywane są z dokładnością co do sekundy. Oferta wraz z załącznikami musi zostać złożona w postaci elektronicznej oraz podpisana kwalifikowanym podpisem elektronicznym, podpisem osobistym lub podpisem zaufanym pod rygorem nieważności. Zamawiający informuje, że podpisanie oferty i innych dokumentów nie następuje na platformie do komunikacji. Wykonawca przygotowuje ofertę przy pomocy interaktywnego „Formularza ofertowego” udostępnionego przez Zamawiającego na Platformie e-Zamówienia i zamieszczonego w podglądzie postępowania w zakładce „Informacje podstawowe”. Zalogowany wykonawca używając przycisku „Wypełnij” widocznego pod „Formularzem ofertowym” zobowiązany jest do zweryfikowania poprawności danych automatycznie pobranych przez system z jego konta i uzupełnienia pozostałych informacji dotyczących wykonawcy/wykonawców wspólnie ubiegających się o udzielenie zamówienia. Następnie wykonawca powinien pobrać „Formularz ofertowy”, zapisać go na dysku komputera użytkownika, uzupełnić pozostałymi danymi wymaganymi przez Zamawiającego i ponownie zapisać na dysku komputera użytkownika oraz podpisać odpowiednim rodzajem podpisu elektronicznego. Uwaga! Nie należy zmieniać nazwy pliku nadanej przez Platformę e-Zamówienia. Zapisany „Formularz ofertowy” należy zawsze otwierać w programie Adobe Acrobat Reader DC. Wykonawca składa ofertę za pośrednictwem zakładki „Oferty/wnioski”, widocznej w podglądzie postępowania po zalogowaniu się na konto Wykonawcy. Po wybraniu przycisku „Złóż ofertę” system prezentuje okno składania oferty umożliwiające przekazanie dokumentów elektronicznych, w którym znajdują się dwa pola drag&drop („przeciągnij” i „upuść”) służące do dodawania plików. Więcej informacji w Specyfikacji Warunków Zamówienia.

3.8.) Zamawiający wymaga sporządzenia i przedstawienia ofert przy użyciu narzędzi elektronicznego modelowania danych budowlanych lub innych podobnych narzędzi, które nie są ogólnie dostępne: Nie**3.12.) Oferta - katalog elektroniczny: Nie dotyczy****3.14.) Języki, w jakich mogą być sporządzane dokumenty składane w postępowaniu:**

polski

3.15.) RODO (obowiązek informacyjny): Informacje o ochronie danych osobowych zamawiający zamieścił w Specyfikacji Warunków Zamówienia.

3.16.) RODO (ograniczenia stosowania): Informacje o ochronie danych osobowych zamawiający zamieścił w Specyfikacji Warunków Zamówienia.

SEKCJA IV – PRZEDMIOT ZAMÓWIENIA

4.1.) Informacje ogólne odnoszące się do przedmiotu zamówienia.

4.1.1.) Przed wszczęciem postępowania przeprowadzono konsultacje rynkowe: Nie

4.1.2.) Numer referencyjny: OR.271.4.2026

4.1.3.) Rodzaj zamówienia: Usługi

4.1.4.) Zamawiający udziela zamówienia w częściach, z których każda stanowi przedmiot odrębnego postępowania: Nie

4.1.8.) Możliwe jest składanie ofert częściowych: Nie

4.1.13.) Zamawiający uwzględnia aspekty społeczne, środowiskowe lub etykiety w opisie przedmiotu zamówienia: Nie

4.2. Informacje szczegółowe odnoszące się do przedmiotu zamówienia:

4.2.2.) Krótki opis przedmiotu zamówienia

Przedmiotem zamówienia jest wykonanie usług z zakresu cyberbezpieczeństwa, obejmujących w szczególności: przeprowadzenie audytu zgodności z Krajowymi Ramami Interoperacyjności oraz audytu zgodności z ustawą o krajowym systemie cyberbezpieczeństwa, opracowanie rejestru ryzyka oraz analizy GAP, opracowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) dla trzech jednostek wskazanych przez Zamawiającego, przeprowadzenie szkoleń z cyberbezpieczeństwa dla pracowników jednostek Gminy oraz dla informatyka, przeprowadzenie audytu bezpieczeństwa w obszarze sieci, serwerów i oprogramowania serwerowego, a także wykonanie testów penetracyjnych infrastruktury informatycznej wraz z identyfikacją podatności oraz testów socjotechnicznych. Szczegółowy Opis Przedmiotu Zamówienia (OPZ) zawiera Załącznik nr 4 do SWZ.

4.2.6.) Główny kod CPV: 72810000-1 - Usługi audytu komputerowego

4.2.7.) Dodatkowy kod CPV:

72000000-5 - Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia

72150000-1 - Usługi doradztwa w zakresie audytu komputerowego oraz sprzętu komputerowego

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: do 2026-09-25

4.2.11.) Zamawiający przewiduje wznowienia: Nie

4.2.13.) Zamawiający przewiduje udzielenie dotychczasowemu wykonawcy zamówień na podobne usługi lub roboty budowlane: Nie

4.3.) Kryteria oceny ofert

4.3.1.) Sposób oceny ofert: Zamawiający stosuje następujące kryteria oceny oferty.

Przy wyborze najkorzystniejszej oferty zamawiający będzie kierował się następującymi kryteriami i odpowiadającymi im znaczeniami oraz w następujący sposób będzie oceniał spełnienie kryteriów:

Oferty będą oceniane metodą punktową w skali 100-punktowej.

1. Cena ofertowa brutto – 60%

Cena będzie oceniana metodą punktową wg wzoru:

Cena najniższa ze wszystkich ofert nieodrzuconych x 100 pkt x Znaczenie kryterium 60% / Cena oferty badanej

Oferta może otrzymać maksymalnie 60 pkt (1% = 1 pkt) w zakresie kryterium ceny.

2. Kryterium „Dysponowanie osobą posiadającą certyfikat OSWE” — waga 30 %

Jeżeli wykonawca wykaże w Wykazie osób do kryterium oceny ofert dysponowanie co najmniej jedną osobą posiadającą ważny certyfikat OSWE (Offensive Security Web Expert) albo certyfikat równoważny, oferta otrzyma 30 punktów. W przypadku niewykazania takiej osoby oferta otrzyma 0 punktów. Osoba wskazana w tym kryterium może być jednocześnie osobą wskazaną na potwierdzenie warunku udziału w postępowaniu.

3. Kryterium „Dysponowanie Kierownikiem Projektu” — waga 10 %

Jeżeli wykonawca wykaże dysponowanie osobą pełniącą funkcję Kierownika Projektu, posiadającą ważny certyfikat PRINCE2 Practitioner albo PMP (Project Management Professional — PMI) albo certyfikat równoważny, oferta otrzyma 10 punktów. W przypadku niewykazania takiej osoby oferta otrzyma 0 punktów.

4. Sposób ustalenia oceny końcowej

Łączna liczba punktów przyznanych ofercie obliczana jest według wzoru:

$$P = P(C) + P(OSWE) + P(KP)$$

gdzie: P — łączna liczba punktów (maksymalnie 100);

P(C) — punkty w kryterium ceny (maksymalnie 60);

P(OSWE) — punkty za dysponowanie osobą posiadającą certyfikat OSWE albo równoważny (30 albo 0);

P(KP) — punkty za dysponowanie Kierownikiem Projektu (10 albo 0).

Za najkorzystniejszą zostanie uznana oferta, która uzyska największą łączną liczbę punktów. Maksymalna liczba punktów możliwych do uzyskania wynosi 100.

4.3.2.) Sposób określania wagi kryteriów oceny ofert: Punktowno

4.3.3.) Stosowane kryteria oceny ofert: Kryterium ceny oraz kryteria jakościowe

Kryterium 1

4.3.5.) Nazwa kryterium: Cena

4.3.6.) Waga: 60,00

Kryterium 2

4.3.4.) Rodzaj kryterium:

organizacja, kwalifikacje zawodowe i doświadczenie osób wyznaczonych do realizacji zamówienia

4.3.5.) Nazwa kryterium: Dysponowanie osobą posiadającą certyfikat OSWE (Offensive Security Web Expert) albo równoważny

4.3.6.) Waga: 30

Kryterium 3

4.3.4.) Rodzaj kryterium:

organizacja, kwalifikacje zawodowe i doświadczenie osób wyznaczonych do realizacji zamówienia

4.3.5.) Nazwa kryterium: Dysponowanie Kierownikiem Projektu posiadającym certyfikat PRINCE2 Practitioner albo równoważny

4.3.6.) Waga: 10

4.3.10.) Zamawiający określa aspekty społeczne, środowiskowe lub innowacyjne, żąda etykiet lub stosuje rachunek kosztów cyklu życia w odniesieniu do kryterium oceny ofert: Nie

SEKCJA V - KWALIFIKACJA WYKONAWCÓW

5.1.) Zamawiający przewiduje fakultatywne podstawy wykluczenia: Nie

5.3.) Warunki udziału w postępowaniu: Tak

5.4.) Nazwa i opis warunków udziału w postępowaniu.

10. Warunki udziału w postępowaniu

Na podstawie art. 112 ustawy Pzp Zamawiający określa następujące warunki udziału w postępowaniu.

Na dzień przygotowania SWZ nie obowiązują przepisy wykonawcze określające poziomy zdolności dla zamówień na usługi, o których mowa w art. 112 ust. 3 ustawy Pzp. Warunki zdolności technicznej lub zawodowej zostały zatem określone bez zastosowania takich poziomów, zgodnie z art. 112 ust. 3 ustawy Pzp.

10.1. Zdolność do występowania w obrocie gospodarczym oraz uprawnienia do prowadzenia działalności

Zamawiający nie określa warunku w tym zakresie.

10.2. Sytuacja ekonomiczna lub finansowa

1. Wykonawca spełni warunek, jeżeli wykaże, że jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia, przy czym ochrona ubezpieczeniowa obejmuje:

– odpowiedzialność cywilną z tytułu świadczenia usług informatycznych i doradczych (OC zawodowa konsultantów IT) — na sumę gwarancyjną nie niższą niż 500 000,00 zł;

– odpowiedzialność cywilną i administracyjną z tytułu naruszenia przepisów o ochronie danych osobowych oraz szkody powstałe w następstwie incydentów cyberbezpieczeństwa — na sumę gwarancyjną nie niższą niż 500 000,00 zł.

2. Dopuszcza się wykazanie powyższych zakresów ochrony w jednej lub w kilku umowach ubezpieczenia.

3. Jeżeli z uzasadnionej przyczyny wykonawca nie może złożyć dokumentów potwierdzających ubezpieczenie, składa inne podmiotowe środki dowodowe, które w wystarczający sposób potwierdzają spełnianie opisanego warunku — zgodnie z § 8 ust. 2 rozporządzenia w sprawie podmiotowych środków dowodowych.

10.3. Zdolność techniczna lub zawodowa — doświadczenie wykonawcy

Wykonawca spełni warunek, jeżeli wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy — w tym okresie, wykonał, a w przypadku świadczeń powtarzających się lub ciągłych również wykonuje, następujące usługi:

4. co najmniej jedną usługę obejmującą łącznie wykonanie testów penetracyjnych infrastruktury teleinformatycznej oraz testów penetracyjnych aplikacji webowej, wraz z analizą zidentyfikowanych podatności, o wartości nie mniejszej niż 40

000,00 zł netto, zrealizowaną na rzecz podmiotu z sektora finansów publicznych;

5. co najmniej jedną usługę obejmującą przeprowadzenie audytu zgodności z Krajowymi Ramami Interoperacyjności lub audytu zgodności z ustawą o krajowym systemie cyberbezpieczeństwa wraz z analizą ryzyka, obejmującą w ramach jednego zamówienia co najmniej 6 jednostek organizacyjnych, o wartości nie mniejszej niż 20 000,00 zł netto, zrealizowaną na rzecz podmiotu z sektora finansów publicznych;

6. co najmniej jedną usługę obejmującą opracowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z normą PN-EN ISO/IEC 27001, o wartości nie mniejszej niż 30 000,00 zł netto;

7. co najmniej pięć szkoleń z zakresu cyberbezpieczeństwa przeprowadzonych na rzecz pięciu różnych jednostek samorządu terytorialnego, przy czym w każdym ze szkoleń uczestniczyło nie mniej niż 20 osób, oraz co najmniej trzy szkolenia specjalistyczne dla administratorów systemów teleinformatycznych w jednostkach samorządu terytorialnego, każde o wymiarze nie mniejszym niż 8 godzin szkoleniowych.

W przypadku usług wykonywanych (świadczenia powtarzające się lub ciągłe) Zamawiający uzna warunek za spełniony, jeżeli zrealizowana część usługi na dzień składania ofert osiągnęła wymaganą wartość i zakres.

Wartości wyrażone w walucie obcej przelicza się według średniego kursu Narodowego Banku Polskiego z dnia publikacji ogłoszenia o zamówieniu.

Zamawiający dopuszcza wykazanie jednej usługi na potwierdzenie więcej niż jednego z warunków określonych w pkt 1–4, o ile usługa ta obejmowała swoim zakresem i wartością wszystkie wskazane elementy.

W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia warunki określone w pkt 1–4 mogą być spełnione łącznie, z zastrzeżeniem art. 117 ust. 3 ustawy Pzp — warunek uważa się za spełniony, jeżeli usługi objęte danym warunkiem wykona ten z wykonawców, który wykazał wymagane w tym zakresie zdolności.

10.4. Zdolność techniczna lub zawodowa — potencjał kadrowy

Wykonawca spełni warunek, jeżeli wykaże, że dysponuje lub będzie dysponował zespołem obejmującym co najmniej następujące osoby:

1. Audytor bezpieczeństwa — co najmniej dwie osoby, z których każda posiada:

– co najmniej 3-letnie doświadczenie w prowadzeniu audytów bezpieczeństwa informacji uwzględniających wymagania

normy ISO/IEC 27001 lub KRI, obejmujące udział w co najmniej dwóch zakończonych zadaniach audytowych;

– co najmniej jeden z certyfikatów wymienionych w załączniku do rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu albo certyfikat równoważny.

2. Pentester — co najmniej dwie osoby, niebędące jednocześnie osobami wskazanymi w roli Audytora bezpieczeństwa, przy czym:

– każda z tych osób posiada co najmniej 3-letnie doświadczenie w wykonywaniu testów bezpieczeństwa technicznego, w tym testów uwzględniających metodykę OWASP oraz brała udział w co najmniej trzech projektach obejmujących testy penetracyjne aplikacji webowych i infrastruktury, z których co najmniej jeden realizowany był na rzecz podmiotu z sektora finansów publicznych;

– każda z tych osób posiada certyfikat OSCP (Offensive Security Certified Professional) albo certyfikat równoważny w rozumieniu rozdziału „Warunki równoważności”;

– co najmniej jedna z tych osób brała udział w co najmniej dwóch projektach obejmujących testy socjotechniczne przeprowadzone na próbie nie mniejszej niż 80 osób w każdym projekcie;

– co najmniej jedna z tych osób posiada certyfikat OSEP (OffSec Experienced Penetration Tester) albo certyfikat równoważny.

3. Trener bezpieczeństwa — co najmniej dwie osoby (dopuszcza się łączenie tej roli z rolą Audytora bezpieczeństwa albo Pentestera), z których każda przeprowadziła co najmniej pięć szkoleń z obszaru cyberbezpieczeństwa dedykowanych jednostkom administracji publicznej, w tym co najmniej dwa szkolenia dotyczące funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji. Szkolenia wykazywane dla poszczególnych trenerów nie mogą się powielać.

Osoby wskazane w wykazie osób zobowiązane są do osobistego wykonywania powierzonych im czynności. Zmiana osoby jest dopuszczalna wyłącznie za uprzednią zgodą Zamawiającego, po wskazaniu przyczyny zmiany oraz osoby o kwalifikacjach i doświadczeniu nie niższych niż wymagane w SWZ. Jeżeli osoba zastępowana była wskazana w Załączniku nr 9 do SWZ i jej kwalifikacje stanowiły podstawę przyznania punktów w kryterium oceny ofert, osoba zastępująca musi zapewniać co najmniej taki sam poziom cechy jakościowej, za który oferta otrzymała punkty; zmiana nie może prowadzić do obniżenia liczby punktów odpowiadającej zaoferowanemu poziomowi jakości.

Spełnianie warunku Zamawiający zweryfikuje na podstawie wykazu osób, o którym mowa w rozdziale „Podmiotowe środki dowodowe składane na wezwanie”. W wykazie należy podać, dla każdego wymaganego certyfikatu, jego nazwę, numer lub identyfikator oraz adres publicznego rejestru albo sposób umożliwiający Zamawiającemu samodzielną weryfikację ważności certyfikatu. Zamawiający nie żąda składania kopii certyfikatów jako podmiotowego środka dowodowego. Okazanie oryginałów certyfikatów przed dopuszczeniem osób do realizacji prac regulują projektowane postanowienia umowy.

10.5. Zdolność techniczna lub zawodowa — system zarządzania bezpieczeństwem informacji wykonawcy

4. Wykonawca spełni warunek, jeżeli wykaże, że posiada wdrożony i certyfikowany system zarządzania bezpieczeństwem informacji zgodny z normą PN-EN ISO/IEC 27001, obejmujący swoim zakresem świadczenie usług z zakresu cyberbezpieczeństwa lub usług informatycznych. Certyfikat musi być wydany dla podmiotu, a nie dla osoby fizycznej.

5. Certyfikat powinien być wydany przez jednostkę certyfikującą akredytowaną przez Polskie Centrum Akredytacji albo przez jednostkę akredytowaną przez krajową jednostkę akredytującą innego państwa członkowskiego Europejskiego Obszaru Gospodarczego, będącą sygnatariuszem wielostronnego porozumienia EA MLA, zgodnie z zasadą wzajemnego uznawania akredytacji wynikającą z rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008.

6. Wykonawca może złożyć równoważne podmiotowe środki dowodowe wystawione przez podmioty mające siedzibę w innym państwie członkowskim Europejskiego Obszaru Gospodarczego (§ 9 ust. 5 rozporządzenia w sprawie podmiotowych środków dowodowych).

7. Wykonawca, który z przyczyn od niego niezależnych nie ma dostępu do certyfikatu lub możliwości uzyskania go w odpowiednim terminie, może złożyć inne podmiotowe środki dowodowe dotyczące stosowanych środków zapewnienia bezpieczeństwa informacji, o ile udowodni, że stosowane przez niego środki są zgodne z wymaganą normą (§ 9 ust. 6 rozporządzenia w sprawie podmiotowych środków dowodowych).

8. W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia warunek uważa się za spełniony, jeżeli certyfikatem albo równoważnymi środkami dowodowymi legitymuje się każdy z wykonawców, który w ramach realizacji zamówienia będzie uzyskiwał dostęp do systemów teleinformatycznych, danych lub informacji Zamawiającego. Wymóg nie dotyczy wykonawcy realizującego wyłącznie czynności niewiążące się z takim dostępem.

5.5.) Zamawiający wymaga złożenia oświadczenia, o którym mowa w art.125 ust. 1 ustawy: Tak

5.6.) Wykaz podmiotowych środków dowodowych na potwierdzenie niepodlegania wykluczeniu: 1. Oświadczenie wykonawcy art. 125 ust 1 ustawy pzp,

2. Oświadczenie wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy, o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2020 r. poz. 1076 i 1086), z innym wykonawcą, który złożył odrębną ofertę, ofertę częściową, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej lub wniosku o dopuszczenie do udziału w postępowaniu niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej;

3. oświadczenia wykonawcy o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy Pzp, w zakresie podstaw wykluczenia wskazanych przez Zamawiającego — składanego na podstawie § 3 rozporządzenia w sprawie podmiotowych środków dowodowych, w tym w zakresie podstaw wykluczenia z 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

5.7.) Wykaz podmiotowych środków dowodowych na potwierdzenie spełniania warunków udziału w postępowaniu: 1.

Wykaz usług wykonanych wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy lub usługi zostały wykonane, oraz załączeniem dowodów określających, czy te dostawy zostały wykonane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy lub usługi zostały wykonane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów - oświadczenie wykonawcy.

2. Wykaz osób skierowanych przez wykonawcę do realizacji zamówienia publicznego, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami;

3. Dokument potwierdzający, że wykonawca jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia ze wskazaniem sumy gwarancyjnej tego ubezpieczenia.

4. zaświadczenia niezależnego podmiotu zajmującego się poświadczaniem zgodności z normą PN-EN ISO/IEC 27001 (certyfikatu systemu zarządzania bezpieczeństwem informacji), obejmującego zakresem świadczenie usług z zakresu cyberbezpieczeństwa lub usług informatycznych, wydane dla podmiotu, albo równoważnych podmiotowych środków dowodowych, o których mowa w rozdziale „Warunki udziału w postępowaniu”.

5.8.) Wykaz przedmiotowych środków dowodowych:

Nie dotyczy

5.9.) Zamawiający przewiduje uzupełnienie przedmiotowych środków dowodowych: Nie

5.11.) Wykaz innych wymaganych oświadczeń lub dokumentów:

Formularz ofertowy,

Wykaz osób do kryterium oceny ofert,

Wykaz elementów ICT,

Oświadczenie wykonawcy o niepodleganiu wykluczeniu oraz o spełnianiu warunków udziału w postępowaniu,

Oświadczenie o aktualności informacji zawartych w oświadczeniu z art. 125 ust. 1 ustawy pzp

Oświadczenie wykonawców wspólnie składających ofertę, jeżeli dotyczy

Wykonawca, który powołuje się na rozwiązania równoważne, jest zobowiązany wykazać, że oferowane przez niego rozwiązanie spełnia wymagania określone przez zamawiającego. W takim przypadku, wykonawca załącza do oferty wykaz rozwiązań równoważnych wraz z jego opisem lub normami.

Pełnomocnictwo

- Gdy umocowanie osoby składającej ofertę nie wynika z dokumentów rejestrowych, wykonawca, który składa ofertę za pośrednictwem pełnomocnika, powinien dołączyć do oferty dokument pełnomocnictwa obejmujący swym zakresem umocowanie do złożenia oferty lub do złożenia oferty i podpisania umowy.

- W przypadku wykonawców ubiegających się wspólnie o udzielenie zamówienia wykonawcy zobowiązani są do ustanowienia pełnomocnika. Dokument pełnomocnictwa, z treści którego będzie wynikało umocowanie do reprezentowania w postępowaniu o udzielenie zamówienia tych wykonawców należy załączyć do oferty.

Pełnomocnictwo powinno być załączone do oferty i powinno zawierać w szczególności wskazanie:

- postępowania o zamówienie publiczne, którego dotyczy,
- wszystkich wykonawców ubiegających się wspólnie o udzielenie zamówienia wymienionych z nazwy z określeniem adresu siedziby,
- ustanowionego pełnomocnika oraz zakresu jego umocowania.

Oświadczenie wykonawców wspólnie ubiegających się o udzielenie zamówienia

- Wykonawcy wspólnie ubiegający się o udzielenie zamówienia, spośród których tylko jeden spełnia warunek dotyczący uprawnień, są zobowiązani złożyć oświadczenie, z którego wynika, które roboty budowlane, dostawy lub usługi wykonają poszczególni wykonawcy.
- Wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z wykonawców, którzy wykonają roboty budowlane lub usługi, do realizacji których te zdolności są wymagane. W takiej sytuacji wykonawcy są zobowiązani dołączyć do oferty oświadczenie, z którego wynika, które roboty budowlane, dostawy lub usługi wykonają poszczególni wykonawcy.

Zobowiązanie podmiotu trzeciego Zobowiązanie podmiotu udostępniającego zasoby lub inny podmiotowy środek dowodowy potwierdza, że stosunek łączący wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:

- zakres dostępnych wykonawcy zasobów podmiotu udostępniającego zasoby;
- sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
- czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane lub usługi, których wskazane zdolności dotyczą.

Zastrzeżenie tajemnicy przedsiębiorstwa (jeżeli dotyczy)

SEKCJA VI - WARUNKI ZAMÓWIENIA

6.1.) Zamawiający wymaga albo dopuszcza oferty wariantowe: Nie

6.3.) Zamawiający przewiduje aukcję elektroniczną: Nie

6.4.) Zamawiający wymaga wadium: Nie

6.5.) Zamawiający wymaga zabezpieczenia należytego wykonania umowy: Nie

6.6.) Wymagania dotyczące składania oferty przez wykonawców wspólnie ubiegających się o udzielenie zamówienia:

Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku:

- Wykonawcy występujący wspólnie są zobowiązani do ustanowienia pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania ich w postępowaniu i zawarcia umowy w sprawie przedmiotowego zamówienia publicznego.
- Wszelka korespondencja będzie prowadzona przez zamawiającego wyłącznie z pełnomocnikiem.

6.7.) Zamawiający przewiduje unieważnienie postępowania, jeśli środki publiczne, które zamierzał przeznaczyć na sfinansowanie całości lub części zamówienia nie zostały przyznane: Nie

SEKCJA VII - PROJEKTOWANE POSTANOWIENIA UMOWY

7.1.) Zamawiający przewiduje udzielenia zaliczek: Nie

7.3.) Zamawiający przewiduje zmiany umowy: Tak

7.4.) Rodzaj i zakres zmian umowy oraz warunki ich wprowadzenia:

1. Zmiana umowy wymaga formy pisemnej pod rygorem nieważności i jest dopuszczalna w przypadkach określonych w art. 455 ustawy Pzp oraz w przypadkach wskazanych poniżej.
2. Zamawiający dopuszcza zmianę terminu wykonania umowy w razie: wystąpienia siły wyższej; okoliczności leżących po stronie Zamawiającego uniemożliwiających prowadzenie prac; konieczności wstrzymania prac ze względu na ryzyko zakłócenia ciągłości działania Zamawiającego — o okres odpowiadający czasowi trwania przeszkody.
3. Zamawiający dopuszcza zmianę zakresu i sposobu realizacji przedmiotu umowy w razie zmiany przepisów prawa mających wpływ na zakres audytów lub dokumentacji SZBI, w szczególności przepisów ustawy o krajowym systemie cyberbezpieczeństwa lub rozporządzenia w sprawie Krajowych Ram Interoperacyjności.
4. Zamawiający dopuszcza zmianę wynagrodzenia w razie ustawowej zmiany stawki podatku od towarów i usług — w zakresie odpowiadającym zmianie stawki, przy niezmienionym wynagrodzeniu netto.

7.5.) Zamawiający uwzględnił aspekty społeczne, środowiskowe, innowacyjne lub etykiety związane z realizacją zamówienia: Nie

SEKCJA VIII – PROCEDURA

8.1.) Termin składania ofert: 2026-08-18 12:00

8.2.) Miejsce składania ofert: Ofertę wraz z wymaganymi dokumentami i oświadczeniami należy złożyć za pośrednictwem

Platformy e-Zamówienia pod adresem: <https://ezamowienia.gov.pl>

8.3.) Termin otwarcia ofert: 2026-08-18 12:30

8.4.) Termin związania ofertą: do 2026-09-01

SEKCJA IX – POZOSTAŁE INFORMACJE

Zamawiający wykluczy z postępowania wykonawców, wobec których zachodzą podstawy wykluczenia, o których mowa w 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. poz. 835) tj.

1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;

2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;

3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy.