

Poniatowa, dnia 15.10.2024

Znak sprawy: INP.7013.52.2024

Zamawiający:Gmina Poniatowa
Ul. Młodzieżowa 2,
24-320 Poniatowa**Zapytanie o cenę**

w celu ustalenia szacunkowej wartości zamówienia

Zapraszamy Państwa do przedstawienia oferty cenowej w celu oszacowania wartości zamówienia pn.: „Przeprowadzenie audytów wstępnych i końcowych systemu zarządzania bezpieczeństwem informacji wraz z usługą testów penetracyjnych, opracowanie nowych polityk i procedur oraz aktualizacja posiadanej dokumentacji SZBI, przeprowadzenie szkoleń stacjonarnych w zakresie bezpieczeństwa informacji oraz cyberbezpieczeństwa dla Urzędu Miejskiego w Poniatowej” w ramach opracowania i wdrożenia - realizowanego w ramach projektu grantowego pn. „Cyberbezpieczny Samorząd” realizowanego w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa”.

1. Propozycję ceny należy składać na formularzu stanowiącym **załącznik nr 1** do niniejszego zapytania w terminie **do dnia 23.10.2024 do godz. 14.00** na adres: inwestycje@um.poniatowa.pl z tematem wiadomości **„Szacowanie wartości zamówienia realizowanego z projektu „Cyberbezpieczny Samorząd” realizowanego w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa”**.
2. Projekt umowy stanowi **załącznik nr 2** do zapytania.
3. Zamawiający **nie przewiduje podziału zamówienia na części**.
4. Zamawiający przewiduje płatności częściowe po realizacji poszczególnych zadań.
5. Zamawiający informuje, że przedmiotowe ogłoszenie nie stanowi oferty w rozumieniu art. 66 ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (tj. Dz. U. 2023 poz.1610 z późn. zm.), ani nie jest ogłoszeniem o zamówieniu w rozumieniu ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tj. Dz. U. z 2023 r., poz. 1605 z późn. zm.). Ma ono na celu wyłącznie oszacowanie wartości zamówienia w związku z planowanym zamówieniem publicznym.
6. Osobą do kontaktu w sprawach dotyczących postępowania jest: Lidia Kuna, e-mail: inwestycje@um.poniatowa.pl tel. 81 820 48 36 w. 15
7. Administratorami danych osobowych przetwarzanych w ramach projektu „Cyberbezpieczny Samorząd” są:

- 7.1 Minister Funduszy i Polityki Regionalnej (dalej jako MFiPR), w zakresie w jakim pełni funkcję Instytucji Zarządzającej (IZ) Funduszami Europejskimi na Rozwój Cyfrowy 2021-2027 (dalej jako FERC) z siedzibą przy ul. Wspólnej 2/4, 00-926 Warszawa,
- 7.2 Centrum Projektów Polska Cyfrowa (dalej jako CPPC) w zakresie w jakim pełni funkcję Instytucji Pośredniczącej (IP) FERC, z siedzibą przy ul. Spokojnej 13A, 01-044 Warszawa,
- 7.3 Centrum Projektów Polska Cyfrowa (dalej jako CPPC) w zakresie w jakim pełni funkcję Beneficjenta FERC, z siedzibą przy ul. Spokojnej 13A, 01-044 Warszawa.
8. Więcej informacji o tym jak przetwarzane są dane osobowe w ramach projektu „Cyberbezpieczny Samorząd” znajduje się w klauzuli informacyjnej FERC stanowiącej załącznik nr 1 do projektu umowy.

9. ZAMÓWIENIE OBEJMUJE 5 ZADAŃ DO WYKONANIA:

Zadanie 1:

Przeprowadzenie audytu wstępnego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie;

Zadanie 2:

Opracowanie nowych polityk i aktualizacja dokumentacji w ramach opracowania i wdrożenia SZBI w Urzędzie;

Zadanie 3:

Przeprowadzenie szkoleń z zakresu bezpieczeństwa informacji oddzielnie:

- a) dla kadry zarządzającej Urzędu;
- b) dla pozostałych pracowników Urzędu;

Zadanie 4:

Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla pracowników Urzędu;

Zadanie 5:

Przeprowadzenie audytu końcowego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie;

OPIS PRZEDMIOTU ZAMÓWIENIA:

I. Zakres prac i szczegóły dotyczące przedmiotu zamówienia DLA ZADANIA 1:

1. Szczegółowe wymagania dotyczące audytu wstępnego:

1.1 Liczba jednostek objętych audytem wstępnymi: 1 – Urząd Miejski w Poniatowej.

1.2 Miejsce przeprowadzenia audytu: siedziba Urzędu

1.3 Ilość wszystkich stacji roboczych: 65 szt.

1.4 Ilość wszystkich serwerów: 3 szt.

1.5 Ilość wszystkich urządzeń sieciowych: 36 szt.

1.6 Zakres audytu wstępnego:

- 1.6.1 Ocena poziomu bezpieczeństwa organizacyjnego związanego z posiadaną dokumentacją i procedurami.
- 1.6.2 Ocena poziomu bezpieczeństwa technicznego związanego z posiadaną infrastrukturą, jej funkcjonowaniem i wydajnością.
- 1.6.3 Przeprowadzenie testów penetracyjnych obejmujących testy styku sieci lokalnej z Internetem (Analiza topologii brzegu sieci, Weryfikacja mechanizmów ochronnych, Próba wykrycia usług sieciowych udostępnianych do Internetu, Detekcja wersji

oraz typu oprogramowania dostępnego z sieci Internet, Exploitacja dostępnych urządzeń oraz usług wystawionych do sieci Internet.

- 1.6.4 Przeprowadzenie testów penetracyjnych ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego (Analiza topologii sieci LAN, Weryfikacja mechanizmów ochronnych w sieci, Analiza komunikacji sieciowej, Skanowanie portów TCP/UDP i próba wykrycia usług sieciowych, Skanowanie hostów aktywnych w sieci, Exploitacja dostępnych urządzeń oraz usług w sieci LAN.
- 1.7 Zakres przeprowadzanego audytu w oparciu o przepisy i normy:
 - 1.7.1 Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
 - 1.7.2 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.
 - 1.7.3 Ustawa o krajowym systemie cyberbezpieczeństwa.
 - 1.7.4 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679
 - 1.7.5 Normy ISO 27001.
- 1.8 Raport z audytu wstępnego musi zawierać informacje o stanie aktualnym, stwierdzonych uchybieniach oraz zalecenia pokontrolne.
- 1.9 Forma przekazania i omówienia raportu: Spotkanie w siedzibie Urzędu podczas którego wyniki audytu zostaną omówione z kadrą kierowniczą.
- 1.10 Wymagania dla wykonawcy:
 - 1.10.1 Wykonawca musi posiadać co najmniej 2 certyfikaty potwierdzające kwalifikacje do przeprowadzenia audytów SZBI zgodnie z Rozporządzeniem Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.
 - 1.10.2 Wykonawca musi posiadać co najmniej 3 letnie, udokumentowane doświadczenie w przeprowadzaniu audytów SZBI i testów penetracyjnych oraz w opracowywaniu raportów pokontrolnych.
 - 1.10.3 Zespół kontrolny musi składać się z co najmniej 2 audytorów posiadających doświadczenie zawodowe i udokumentowaną wiedzę zarówno w kwestiach organizacyjno-prawnych w zakresie audytowania systemów zarządzania bezpieczeństwem informacji, jak i technicznych aspektów bezpieczeństwa IT w zakresie wykonywania testów penetracyjnych, co dodatkowo zostanie potwierdzone certyfikatem branżowym lub wykształceniem np. w postaci dyplomu ukończenia szkoły wyższej o kierunkach związanych z bezpieczeństwem informacji oraz informatyką.
- 1.11 Terminy realizacji zamówienia: Zgodnie z projektem umowy.

2 Zakres prac i szczegóły dotyczące przedmiotu zamówienia DLA ZADANIA 2:

Opracowanie nowych polityk i aktualizacja dokumentacji w ramach wdrożenia SZBI

- 1.1 Liczba jednostek objętych zamówieniem: 1 Urząd Miejski w Poniatowej.
- 1.2 Obecny stan dokumentacji SZBI: Wymagane jest opracowanie nowych polityk oraz aktualizacja istniejącej dokumentacji.

- 1.3 Podział dokumentacji: Wymagany jest podział dokumentacji na 4 części (Polityka Bezpieczeństwa Informacji, Polityka Bezpieczeństwa Danych Osobowych, Polityka Bezpieczeństwa Systemów Informatycznych, Polityka Bezpieczeństwa Fizycznego)
- 1.4 Obszary które powinny zostać objęte szczególnym uwzględnieniem w dokumentacji:
- a) Cel i zakres polityk w kontekście bezpieczeństwa informacji (BI);
 - b) Role i odpowiedzialności pracowników w zakresie BI;
 - c) Zarządzanie ryzykiem w obszarze BI;
 - d) Procedury zarządzania incydentami BI;
 - e) Deklarację stosowania zabezpieczeń;
 - f) Kontrole dostępu do informacji i zasobów;
 - g) Procedury związane z tworzeniem i prowadzeniem aktyw informacyjnych;
 - h) Zasady pracy na odległość i mobilny dostęp do informacji;
 - i) Bezpieczeństwo fizyczne pomieszczeń i obiektów związanych z BI;
 - j) Bezpieczeństwo fizyczne nośników informacji;
 - k) Bezpieczeństwo infrastruktury wspomagającej;
 - l) Inwentaryzacja systemów informacyjnych;
 - m) Zarządzanie bezpieczeństwem i ciągłością działania łańcuch dostaw;
 - n) Projektowanie i wdrażanie systemów teleinformatycznych;
 - o) Kopie zapasowe i zarządzanie ciągłością działania;
 - p) Sprzęt komputerowy, oprogramowanie strategiczne systemy i aplikacje;
 - q) Serwery, informatyczna sieć wewnętrzna;
 - r) Rozliczalność działań w systemach informatycznych;
 - s) Procedury uwzględnienia BI w procesach planowania i zarządzania ciągłością działania;
 - t) Procedury bezpieczeństwa informacji w relacjach z dostawcami;
 - u) Okresowe szkolenia i podnoszenie świadomości pracowników z zakresu BI;
 - v) Cykliczne audyty i monitorowanie SZBI.
- 1.5 Dokumentacja musi zostać opracowana z uwzględnieniem przepisów RODO, ISO 27001, ustawy o krajowym systemie cyberbezpieczeństwa oraz rozporządzenia w sprawie krajowych ram interoperacyjności.
- 1.6 Indywidualizacja dokumentacji Dokumentacja musi być opracowana z uwzględnieniem wymagań i potrzeb stron zainteresowanych (wewnętrznych i zewnętrznych), opracowana na podstawie przepisów oraz informacji udzielonych przez pracowników podczas spotkań projektowych.
- 1.7 Wymagania dotyczące spotkań projektowych Liczba spotkań projektowych wynosi minimum 2-3 udokumentowane spotkania z kadrą kierowniczą. Spotkania te mają na celu zebranie informacji niezbędnych do opracowania indywidualnych procedur oraz omówienie specyficznych potrzeb i wymagań Urzędu.
- 1.8 Termin zakończenia prac nad dokumentacją: Zgodnie z projektem umowy
- 1.9 Raportowanie i zatwierdzenie dokumentacji:
- 1.9.1 Po opracowaniu dokumentacji, wykonawca prześle projekt do zatwierdzenia kierownictwu.
 - 1.9.2 W przypadku zgłoszenia zmian lub poprawek wykonawca zobligowany jest do naniesienia poprawek lub przedstawienia pisemnych wyjaśnień w ciągu 14 dni.
- 1.10 Aktualizacja dokumentacji: Wykonawca zobligowany jest do przeglądu i aktualizacji opracowanej dokumentacji po zrealizowaniu i wdrożeniu zakupów objętych projektem

Cyberbezpieczny samorząd na wezwanie Zamawiającego w terminie 14 dni od otrzymania wezwania.

3 Zakres prac i szczegóły dotyczące przedmiotu zamówienia DLA ZADANIA 3:

1. Szczegółowe wymagania dotyczące szkoleń z zakresu bezpieczeństwa informacji

1.1 Zakres i cel szkoleń:

- 1.1.1 Szkolenie będzie obejmowało szczegółowe omówienie opracowanej dokumentacji SZBI.
- 1.1.2 Celem szkoleń jest zwiększenie świadomości pracowników, zapewnienie zgodności z przepisami oraz wdrożenie nowych procedur bezpieczeństwa informacji.
- 1.1.3 Szkolenia obejmują tematykę związaną z RODO, bezpieczeństwem informacji, zarządzaniem incydentami, korzystaniem z urządzeń mobilnych, postępowaniem z nośnikami danych, kontrolą dostępu, zabezpieczaniem pomieszczeń i obiektów, czystym biurkiem, czystym ekranem, wykonywaniem kopii zapasowych, ochroną logów, bezpieczeństwem komunikacji, zarządzaniem bezpieczeństwem sieci, przesyłaniem informacji, opracowywaniem planów ciągłości działania, zarządzaniem incydentami bezpieczeństwa informacji, ochroną danych osobowych, szacowaniem ryzyka w obszarze bezpieczeństwa informacji oraz okresowymi szkoleniami personelu.

1.2 Liczba uczestników i grup szkoleniowych:

- 1.2.1 Całkowita liczba uczestników szkolenia: 50 pracowników Urzędu.
- 1.2.2 Liczba grup szkoleniowych: Minimum 4 grupy aby uniknąć dezorganizacji normalnej pracy Urzędu
- 1.2.3 Podział na grupy: Kadra zarządzająca oraz pozostali pracownicy.

1.3 Forma szkoleń:

- 1.3.1 Szkolenia stacjonarne w siedzibie Urzędu.
- 1.3.2 Metody szkoleniowe: wykłady, warsztaty, ćwiczenia praktyczne.
- 1.3.3 Czas trwania szkolenia dla jednej grupy: 3 - 4 godziny.
- 1.3.4 Szkolenia odbywać się będą od poniedziałku do piątku w godzinach 8:00-15:00.

1.4 Materiały szkoleniowe:

- 1.4.1 Wykonawca zapewni materiały szkoleniowe w formie prezentacji, ćwiczeń oraz podręczników.
- 1.4.2 Materiały będą dostępne zarówno w formie drukowanej, jak i elektronicznej.

1.5 Wymagania dotyczące wykonawcy

- 1.5.1 Trenerzy muszą posiadać odpowiednie kwalifikacje i doświadczenie w prowadzeniu szkoleń z zakresu bezpieczeństwa informacji.
- 1.5.2 Preferowane certyfikaty i akredytacje trenerów.
- 1.5.3 Wykonawca musi posiadać certyfikat firmy szkoleniowej lub udokumentować przynależność do branżowych organizacji szkoleniowych.

1.6 Konspekt szkolenia:

- 1.6.1 Wykonawca opracuje szczegółowy konspekt szkolenia i przedstawi do akceptacji zamawiającemu.
- 1.6.2 Zamawiający zastrzega sobie prawo do zmiany, uwagi i sugestii dotyczących programu szkolenia

1.7 Ewaluacja szkoleń:

- 1.7.1 Wykonawca zapewni ewaluację szkoleń poprzez testy wiedzy i ankiety satysfakcji uczestników.
- 1.7.2 Wymagane jest przeprowadzenie pretestu przed rozpoczęciem szkolenia w celu oceny początkowego poziomu wiedzy uczestników.

- 1.7.3 Wymagane jest przeprowadzenie posttestu po zakończeniu szkolenia w celu oceny zdobytej wiedzy i efektywności szkolenia.
- 1.7.4 Wyniki ewaluacji będą uwzględnione w końcowym raporcie.
- 1.7.5 Po zakończeniu szkolenia każdy uczestnik otrzyma certyfikat uwzględniający zakres szkolenia oraz potwierdzający udział i zdobyte umiejętności.
- 1.8 Termin szkolenia: Zgodnie z projektem umowy.

4 Zakres prac i szczegóły dotyczące przedmiotu zamówienia DLA ZADANIA 4:

- 1. Szczegółowe wymagania dotyczące szkoleń z zakresu cyberbezpieczeństwa
 - 1.1 Zakres i cel szkoleń:
 - 1.1.1 Celem szkoleń jest zwiększenie świadomości zagrożeń, edukowanie uczestników o aktualnych zagrożeniach cybernetycznych, takich jak phishing, ransomware, malware, ataki DDoS i inne rodzaje cyberataków. Zrozumienie, jak te zagrożenia mogą wpływać na organizację oraz jakie mogą być konsekwencje ich wystąpienia.
 - 1.1.2 Minimalny zakres tematyczny szkoleń musi nawiązywać do wprowadzenia do zagadnień związanych z cyberbezpieczeństwem, zarządzanie incydentami bezpieczeństwa cyfrowego, ochrona przed zagrożeniami cyfrowymi, bezpieczeństwo sieci i infrastruktury IT, zarządzanie hasłami i uwierzytelnianiem, bezpieczne korzystanie z urządzeń mobilnych, postępowanie z nośnikami danych, tworzenie i zarządzanie kopiami zapasowymi, ochrona logów systemowych, zarządzanie bezpieczeństwem sieci, przesyłanie informacji, szacowanie ryzyka w obszarze bezpieczeństwa informacji
 - 1.2 Liczba uczestników i grup szkoleniowych: 50 pracowników Urzędu.
 - 1.3 Liczba grup szkoleniowych: Minimum 3 grupy aby uniknąć dezorganizacji normalnej pracy Urzędu.
 - 1.4 Forma szkoleń:
 - 1.4.1 Szkolenia stacjonarne w siedzibie Urzędu.
 - 1.4.2 Metody szkoleniowe: Wykłady, warsztaty, ćwiczenia praktyczne.
 - 1.4.3 Czas trwania szkolenia dla jednej grupy: 3 - 4 godziny.
 - 1.4.4 Szkolenia odbywać się będą od poniedziałku do piątku w godzinach 8:00-15:00.
 - 1.5 Materiały szkoleniowe:
 - 1.5.1 Wykonawca zapewni materiały szkoleniowe w formie prezentacji, ćwiczeń oraz podręczników.
 - 1.5.2 Materiały będą dostępne zarówno w formie drukowanej, jak i elektronicznej.
 - 1.6 Wymagania dotyczące kwalifikacji trenerów:
 - 1.6.1 Trenerzy muszą posiadać odpowiednie kwalifikacje i doświadczenie w prowadzeniu szkoleń z cyberbezpieczeństwa.
 - 1.6.2 Preferowane certyfikaty i akredytacje trenerów.
 - 1.6.3 Wykonawca musi posiadać certyfikat firmy szkoleniowej lub udokumentować przynależność do branżowych organizacji szkoleniowych.
 - 1.7 Konspekt szkolenia:
 - 1.7.1 Wykonawca opracuje szczegółowy konspekt szkolenia i przedstawi do akceptacji zamawiającemu.
 - 1.7.2 Zamawiający zastrzega sobie prawo do zmiany, uwagi i sugestii dotyczących programu szkolenia
 - 1.8 Ewaluacja szkoleń:
 - 1.8.1 Wykonawca zapewni ewaluację szkoleń poprzez testy wiedzy i ankiety satysfakcji uczestników.

- 1.8.2 Wymagane jest przeprowadzenie pretestu przed rozpoczęciem szkolenia w celu oceny początkowego poziomu wiedzy uczestników.
- 1.8.3 Wymagane jest przeprowadzenie posttestu po zakończeniu szkolenia w celu oceny zdobytej wiedzy i efektywności szkolenia.
- 1.8.4 Wyniki ewaluacji będą uwzględnione w końcowym raporcie.
- 1.8.5 Po zakończeniu szkolenia każdy uczestnik otrzyma certyfikat uwzględniający zakres szkolenia oraz potwierdzający udział i zdobyte umiejętności.
- 1.9 Termin szkolenia: Zgodnie z projektem umowy.

5 Zakres prac i szczegóły dotyczące przedmiotu zamówienia DLA ZADANIA 5:

1. Szczegółowe wymagania dotyczące audytu końcowego:

- 1.1 Liczba jednostek objętych audytami końcowymi: 1 – Urząd Miejski w Poniatowej
- 1.2 Miejsce przeprowadzenia audytu końcowego: siedziba Urzędu Miejskiego w Poniatowej
- 1.3 Zakres audytu końcowego:
 - 1.3.1 Ocena poziomu bezpieczeństwa organizacyjnego związanego z posiadaną dokumentacją i procedurami.
 - 1.3.2 Ocena poziomu bezpieczeństwa technicznego związanego z posiadaną infrastrukturą, jej funkcjonowaniem i wydajnością.
 - 1.3.3 Przeprowadzenie testów obejmujących konfigurację zakupionych w ramach projektu grantowego urządzeń i oprogramowania zwiększającego poziom bezpieczeństwa cyfrowego
- 1.4 Zakres audytu przeprowadzony będzie na podstawie przepisów:
 - 1.4.1 Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
 - 1.4.2 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.
 - 1.4.3 Ustawa o krajowym systemie cyberbezpieczeństwa.
 - 1.4.4 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679
 - 1.4.5 Normy ISO 27001.
- 1.5 Raport z audytu końcowego musi zawierać co najmniej informacje o tym jak zakupy w ramach projektu wpłynęły na poprawę bezpieczeństwa informacji i cyberbezpieczeństwa w Urzędzie.
- 1.6 Forma przekazania i omówienia raportu: Spotkanie w siedzibie Urzędu podczas którego wyniki audytu zostaną omówione z kadrą kierowniczą.
- 1.7 Wymagania dla wykonawcy:
 - 1.7.1 Wykonawca musi posiadać co najmniej 2 certyfikaty potwierdzające kwalifikacje do przeprowadzenia audytów SZBI zgodnie z Rozporządzeniem Ministra Cyfryzacji z dnia 12 października 2018 r.
 - 1.7.2 Wykonawca musi posiadać co najmniej 3 letnie, udokumentowane doświadczenie w przeprowadzaniu audytów SZBI i testów penetracyjnych oraz w opracowywaniu raportów pokontrolnych.
 - 1.7.3 Zespół kontrolny musi składać się z co najmniej 2 audytorów posiadających doświadczenie zawodowe i udokumentowaną wiedzę zarówno w kwestiach organizacyjno-prawnych w zakresie audytowania systemów zarządzania

bezpieczeństwem informacji, jak i technicznych aspektów bezpieczeństwa IT w zakresie wykonywania testów penetracyjnych, co dodatkowo zostanie potwierdzone certyfikatem branżowym lub wykształceniem np. w postaci dyplomu ukończenia szkoły wyższej o kierunkach związanych z bezpieczeństwem informacji oraz z informatyką.

1.8 Terminy realizacji zamówienia: Zgodnie z projektem umowy.

Załączniki do zapytania:

1. Nr 1 – Formularz ofertowy;
2. Nr 2 – Projekt umowy.

