Cyberbezpieczny Samorząd

ZAPYTANIE OFERTOWE

prowadzone zgodnie z zasadą konkurencyjności o wartości poniżej kwoty 130.000 zł na realizację zadania pn.:

usług wsparcia w przygotowaniu i realizacji projektu, realizowanych przez zewnętrznych ekspertów z zakresu cyberbezpieczeństwa posiadających niezbędne kwalifikacje w ramach projektu grantowego pn. „Cyberbezpieczna Gmina Police (skrót CGP)" dofinansowanego z projektu z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027

1. Zamawiający:

Gmina Police
ul. Stefana Batorego 3,
72-010 Police,
NIP: 851-10-00-695,

2. Szczegółowy zakres zamówienia obejmuje:

Wspólny słownik zamówień (CPV):

- Usługi doradcze w zakresie bezpieczeństwa - 79417000-0
- Usługi opracowywania oprogramowania do zarządzania systemem - 72212781-7
- Usługi opracowywania oprogramowania informatycznego - 72212517-6

3. Opis przedmiotu zamówienia:

3.1. Przedmiotem zamówienia jest wykonanie przez zewnętrznych ekspertów usług wsparcia dotyczących projektu „Cyberbezpieczna Gmina Police (skrót CGP)" dofinansowanego z projektu z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027; Priorytet II: Zaawansowane usługi cyfrowe; Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, zgodnie z Regulaminem Konkursu Grantowego „Cyberbezpieczny Samorząd"

3.2. Do szczegółowych obowiązków Wykonawcy należeć będzie:

1. Wykonanie usług doradczych w zakresie opracowania i wdrożenia SZBI oraz przeprowadzenie analizy ryzyka obejmujące w szczególności:
   1) Opracowanie, wdrożenie, przegląd, aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji – SZBI.
   2) Opracowanie i wdrożenie procedury identyfikacji, szacowania i tolerowania ryzyk

2. Wdrożenie aplikacji SaaS łącznie z usługami szkoleniowymi:
   1) Usług udostępnienia aplikacji w chmurze obliczeniowej typu SaaS służącej do dystrybucji, aktualizacji i wdrożenia dokumentacji cyberbezpieczeństwa i analizy ryzyka wykonanej w ramach etapu I.
   2) Szkolenie z zakresu cyberbezpieczeństwa dla przedstawicieli kadry zarządzającej JST z zarządzania i oceny ryzyk bezpieczeństwem informacji (Szkolenia dla 30 przedstawicieli kadry zarządzającej Urzędu Miejskiego w Policach, w tym 15 K, 15 M);

3.3. Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji - SZBI powinna być opracowana w oparciu o wykonane analizy, Polską Normę PN-ISO/IEC 27001, ustawę o Krajowym Systemie Cyberbezpieczeństwa, dyrektywę NIS2 i Rozporządzenie Parlamentu Europejskiego RODO, ustawę o informatyzacji podmiotów realizujących zadania publiczne oraz przepisy wykonawcze

3.4. Minimalny zakres dokumentacji SZBI zwierające niezbędne polityki i procedury, w szczególności:

1. Polityka Bezpieczeństwa Informacji;
2. Procedura zarządzania ryzykiem;
3. Instrukcja Zarządzania Systemem Informatycznym;

4. Procedury zarzadzania uprawnieniami;
5. Procedura zarządzania zdalnym dostępem;
6. Procedura szyfrowania danych;
7. Procedury zarządzania kopiami zapasowymi;
8. Polityka czystego biurka i ekranu;
9. Procedura dostępu fizycznego do pomieszczeń;
10. Procedura postępowania z incydentami bezpieczeństwa;
11. Plan ciągłości działania.

3.5. Wykonawca musi zapewnić oprogramowanie w formie usługi SaaS służące do dystrybucji, aktualizacji i wdrożenia dokumentacji cyberbezpieczeństwa i analizy ryzyka w funkcjonalności opisanej w Załączniku nr 5- Opis funkcjonalny aplikacji udostępnionej w chmurze obliczeniowej.

3.6. W ramach usług serwisowych do udostępnionego oprogramowania Wykonawca musi zapewnić usługi:
1. Indywidualne dostosowanie systemu do potrzeb Zamawiającego klienta (do 20 roboczogodzin);
2. Konsultacje techniczne realizowane przez dział wsparcia (do 20 roboczogodzin);
3. Administracja użytkownikami (do 6 roboczogodzin);
4. Szkolenia dodatkowe (do 5 roboczogodzin);
5. Automatyczny backup wykonywany codziennie (do 6 roboczogodzin);
6. Aktualizacja systemu do nowych przepisów (do 6 roboczogodzin);
7. Hosting w chmurze obliczeniowej (SaaS) (do 5GB HDD);
8. Bieżący serwis oprogramowania informatycznego, obejmujący usuwanie błędów i usterek (błędy krytyczne, uniemożliwiające działanie systemu usuwane.

4. Wymagany termin realizacji zamówienia:

4.1. Termin opracowania, wdrożenia, przeglądu, aktualizacji dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji – SZBI oraz procedury identyfikacji, szacowania i tolerowania ryzyk do 4 miesięcy od podpisania umowy.

4.2. Termin udostępnienia aplikacji w chmurze obliczeniowej typu SaaS: od odbioru etapu I do dnia 30.06.2026 r.

4.3. Termin przeprowadzenia szkoleń: od odbioru etapu I do dnia 30.06.2026 r.

5. Wymagania obligatoryjne stawiane Wykonawcom

Zamawiający wymaga, aby Wykonawca spełniał następujące wymagania:

5.1. Wykonawca musi w trakcie realizacji umowy zapewnić Zespół projektowy złożony min. z 6 specjalistów:
1. Kierownik zespołu projektowego
2. Audytor wew. bezpieczeństwa informacji
3. Specjalista ds. technicznych.
4. Specjalista ds. programowania,
5. Specjalista ds. wdrożenia,
6. Specjalista ds. komunikacji.

5.2. Kierownik zespołu projektowego, który będzie przeprowadzić proces audytu, musi posiadać min. doświadczenie:
1. Wiedza z zakresu prowadzenia procesu projektowego lub cyklu projektowego zatwierdzonego przez Komisję Europejską, potwierdzoną certyfikatem PRINCE2 Practitioner /lub równoważnym certyfikatem potwierdzającym umiejętność prowadzenia projektu w metodologii PRINCE2.
2. Wiedza z zakresu funkcjonowania procesów bezpieczeństwa w administracji publicznej
3. Wykształcenie wyższe informatyczne,
4. Umiejętność i doświadczenie w kierowaniu zespołami w projektach zrealizowanych z udziałem środków zewnętrznych,

5.3. Audytor wew. bezpieczeństwa informacji, który będzie przeprowadzić audyt bezpieczeństwa, musi posiadać uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu. Wykaz certyfikatów wskazanych w w/w rozporządzeniu znajduje się poniżej:

1. Certified Internal Auditor (CIA)
2. Certified Information System Auditor (CISA)
3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób
4. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób
5. Certified Information Security Manager (CISM)
6. Certified in Risk and Information Systems Control (CRISC)
7. Certified in the Governance of Enterprise IT (CGEIT)
8. Certified Information Systems Security Professional (CISSP)
9. Systems Security Certified Practitioner (SSCP)
10. Certified Reliability Professional
11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

5.4. Specjalista ds. technicznych - odpowiedzialny za opracowanie i weryfikację zabezpieczeń technicznych musi posiadać min. doświadczenie:

1. Wykształcenie wyższe informatyczne;
2. Doświadczenie polegające na udziale jako ekspert techniczny- w okresie ostatnich 3 lat przed upływem terminu składania ofert -w co najmniej dwóch zakończonych audytach bezpieczeństwa systemów informatycznych połączonych z opracowaniem zabezpieczeń systemów teleinformatycznych;
3. Doświadczenie w pracy zespołowej w projektach zrealizowanych z udziałem środków zewnętrznych.

5.5. Specjalista ds. programowania - odpowiedzialny za programowanie rozwiązań chmurowych związanych z SZBI:

1. Wykształcenie wyższe informatyczne;
2. Doświadczenie polegające na udziale jako programowania aplikacji chmurowych w okresie ostatnich 3 lat przed upływem terminu składania ofert -w co najmniej 5 projektach dotyczących systemów informatycznych dedykowanych dla administracji publicznej;
3. Doświadczenie w pracy zespołowej w projektach zrealizowanych z udziałem środków zewnętrznych

5.6. Specjalista ds. wdrażania - odpowiedzialny za wdrażanie rozwiązań chmurowych związanych z SZBI:

1. Wykształcenie wyższe informatyczne;
2. Doświadczenie polegające na udziale jako wdrożeniu aplikacji chmurowych w okresie ostatnich 3 lat przed upływem terminu składania ofert -w co najmniej 5 projektach dotyczących systemów informatycznych dedykowanych dla administracji publicznej;
3. Doświadczenie w pracy zespołowej w projektach zrealizowanych z udziałem środków zewnętrznych.

5.7. Specjalista ds. komunikacji – odpowiedzialny za koordynację i logistykę prac zespołów projektowych oraz modelowanie kluczowych procesów biznesowych zarządzania bezpieczeństwem informacji:

1. Wykształcenie wyższe;
2. Doświadczenie z okresu ostatnich 3 lat przed upływem terminu składania ofert w pracy zespołowej w projektach zrealizowanych z udziałem środków zewnętrznych.
3. Doświadczenie w zakresie koordynacji i logistyki prac zespołów projektowych i serwisowych.
4. Wiedza z zakresu modelowania procesów biznesowych w notacji BPMN, potwierdzona stosownym certyfikatem.

5.8. Zamawiający dopuszcza łączenia funkcji maksymalnie dla 2 stanowisk, o których mowa w pkt. 5.2,5.3, 5.4. Personel wykonawcy realizujący przedmiot zamówienia musi mieć udokumentowane i potwierdzone doświadczenie i kompetencje wykazane w **Załączniku nr 4.** - Wykaz osób skierowanych przez Wykonawcę do realizacji zamówienia.

5.9. Zamawiający wymaga, aby Wykonawca wykazał, że przeprowadził minimum 1 audyt stanu bezpieczeństwa informatycznego dla jednostek organizacyjnych administracji publicznej.

5.10. Zamawiający wymaga, aby Wykonawca wykazał, że wdrożył aplikację chmurową wspomagających zarządzanie bezpieczeństwem informacji w min. w 1 JST.

5.11. W celu potwierdzenia spełniania przez Wykonawcę warunków udziału w postępowaniu, Zamawiający żąda przedstawienia wykazu usług wykonanych w okresie ostatnich 5 latach przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, daty wykonania i podmiotów, na rzecz których usługi zostały wykonane (zgodnie z **Załącznikiem nr 3** - Wykaz zrealizowanych usług), z załączeniem dowodów określających czy te usługi zostały wykonane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi były wykonywane;

5.12. Wykonawcy, którzy nie wykażą spełnienia warunków udziału w postępowaniu podlegać będą wykluczeniu z udziału w postępowaniu. Ofertę wykonawcy wykluczonego uznaje się za odrzuconą.

6. Kryteria oceny ofert :

Przy wyborze najkorzystniejszej oferty Zamawiający będzie kierował się następującymi kryteriami oceny:
A - CENA (podstawą wyliczeń będzie cena brutto)– 70% (max. 70 pkt.);
B - DOŚWIADCZENIE – 30% (max. 30 pkt.);

7. Opis sposobu przyznawania punktów.

7.1. Sposób oceny ofert w kryterium CENA:

Ilość punktów dla każdej oferty w tym kryterium zostanie wyliczona wg poniższego wzoru:

$$C = \frac{C\ min.}{C\ bad.} \times 70\ \%$$

1 % - 1 punkt

Gdzie:
C – ilość punktów oferty badanej
C min. – cena minimalna spośród wszystkich ofert niepodlegających odrzuceniu
C bad. – cena oferty badanej
Obliczenia dokonywane będą do dwóch miejsc po przecinku.
Maksymalnie w tym kryterium można otrzymać 70 punktów.

7.2. Sposób oceny ofert w kryterium DOŚWIADCZENIE

Doświadczenie Wykonawcy z ostatnich lat oceniane będzie zgodnie z poniższą tabelą:

Doświadczenie	Punktacja przyznana
Przeprowadzenie minimum 1 audytu stanu bezpieczeństwa informatycznego	0 pkt
Wdrożenie aplikacji chmurowych wspomagających zarządzanie bezpieczeństwem informacji w 1 JST	0 pkt
Przeprowadzenie minimum 3 audytów stanu bezpieczeństwa informatycznego dla jednostek organizacyjnych administracji publicznej	10 pkt
Wdrożenie aplikacji chmurowych wspomagających zarządzanie bezpieczeństwem informacji w 2 JST	10 pkt
Wdrożenie aplikacji chmurowych wspomagających zarządzanie bezpieczeństwem informacji w ponad 3 JST	20 pkt

Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w Zapytaniu ofertowym, oraz uzyska najwyższą liczbę punktów obliczoną według poniższego wzoru.
Pc = C +D

Pc – Całkowita liczba punktów uzyskanych przez badaną ofertę. C – Całkowita liczba punktów uzyskana przez badaną ofertę w kryterium „Cena ”; D – Całkowita liczba punktów uzyskana przez badaną ofertę w kryterium „Doświadczenie Wykonawcy”;
Wartość punktowa zostanie podana z dokładnością do dwóch miejsc po przecinku, a zaokrąglenie zostanie dokonane zgodnie z ogólnie przyjętymi zasadami matematyki.
W przypadku, gdy oferty Wykonawców przedstawiają taki sam bilans kryterium ceny i pozostałych kryteriów, za ofertę korzystniejszą zostanie uznana oferta Wykonawcy z zaoferowaną niższą ceną.

8. Termin składania ofert:

Ofertę należy złożyć do dnia 18.10.2024 r. do godziny 10.00. poprzez stronę internetową dla systemu Baza Konkurencyjności 2021 pod linkiem:
https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl, zgodnie z Instrukcją oferenta w BK2021 zamieszczoną na stronie internetowej, pod linkiem https://archiwum-bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/info/web_instruction

9. Istotne dla zamawiającego postanowienia

9.1. Wzór umowy stanowi **załącznik nr 1** do Zapytania ofertowego otwartego.

9.2. Cenę oferty należy podać w złotych polskich z dokładnością do dwóch miejsc po przecinku zgodnie z **załącznikiem nr 2** - Formularz ofertowy. Łączna cena oferty musi obejmować cały zakres zamówienia, określony w zapytaniu ofertowym.

9.3. W cenie oferty należy uwzględnić także inne koszty o ile Oferent je przewiduje (np. koszty dojazdu, opłaty, ubezpieczenia itp.). Przy obliczaniu ceny należy uwzględnić, że cena będzie obowiązywać strony przez cały okres realizacji zamówienia. Jeżeli złożono ofertę, której wybór prowadziłyby do powstania obowiązku podatkowego Zamawiającego, zgodnie z przepisami o podatku od towarów i usług w zakresie dotyczącym wewnątrzwspólnotowego nabycia towarów, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek wpłacić zgodnie z obowiązującymi przepisami.

10. Informacje dodatkowe:

10.1. Postępowanie może zostać zamknięte bez dokonania wyboru, w szczególności w przypadku, gdy oferta najkorzystniejsza, przekracza kwotę jaką Zamawiający może przeznaczyć na sfinansowanie zamówienia. Postępowanie może zostać zamknięte bez wybrania którejkolwiek oferty.

10.2. Zamawiający zastrzega sobie możliwość prezentacji aplikacji do dystrybucji, aktualizacji i wdrożenia dokumentacji cyberbezpieczeństwa i analizy ryzyka.

10.3. Każdy podmiot może złożyć tylko jedna ofertę.

10.4. Nie dopuszcza się składania ofert wariantowych.

10.5. Nie dopuszcza się składania ofert częściowych.

11. Załączniki (wzory dokumentów) które mają być złożone w ramach oferty:

Załącznik nr 2 - Formularz ofertowy
Załącznik nr 3 - Wykaz wykonanych usług
Załącznik nr 4 – Wykaz osób skierowanych przez Wykonawcę do realizacji zamówienia
Załącznik nr 6 – Powiązania kapitałowe
Załącznik nr 7 – Zobowiązanie podmiotu udostępniającego zasoby (opcja)
Odpis lub informację z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru, w celu potwierdzenia, że osoba działająca w imieniu Wykonawcy jest umocowana do jego reprezentowania. Wykonawca nie jest zobowiązany do złożenia odpisu lub informację z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej, jeżeli Zamawiający może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, o ile Wykonawca wskaże Zamawiającemu, wraz ze składaną ofertą, dane umożliwiające dostęp do tych dokumentów.