Realizacja w ramach umowy o powierzenie grantu o numerze:  
FERC.02.02-CS.01-001/23/0013/   
FERC.02.02-CS.01-001/23/2024

Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC)  
Priorytet II: Zaawansowane usługi cyfrowe   
Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa   
Konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd”  
o numerze FERC.02.02-CS.01-001/23

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**„Opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji”**

1. **Przedmiot zamówienia:**

Urząd Miasta Opola realizuje projekt „Cyberbezpieczny Samorząd - podniesienie poziomu bezpieczeństwa i jakości świadczonych usług Urzędu Miasta Opola”, którego celem jest zwiększenie poziomu bezpieczeństwa przetwarzanych informacji oraz systemów informatycznych Urzędu poprzez opracowanie szczegółowych uregulowań w zakresie bezpieczeństwa informacji spełniających niżej wymienione wymagania:

* + rozporządzenia 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.
  + ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
  + Dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (tzw. Dyrektywa NIS 2).

Przedmiotem zamówienia jest opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (zwanego dalej SZBI) spełniającego wymagania norm rodziny ISO 27000 w zakresie bezpieczeństwa informacji, zgodnego z wymaganiami aktualnych norm PN-EN ISO/IEC 27001 oraz zaleceniami aktualnych norm PN-ISO/IEC 27002, PN-ISO-27005 i ISO 31000 w zakresie zarządzania ryzykiem, oraz Systemu Zarządzania Ciągłością Działania w zakresie systemów teleinformatycznych (zwanego dalej BCM) w Urzędzie zgodnego z normą PN-EN ISO 22301.

Opracowany przez Wykonawcę SZBI nie będzie obejmował ochrony informacji niejawnych określonych w ustawie o ochronie informacji niejawnej.

Wykonawca zobowiązany jest opracować spójne, jednolite i adekwatne do ryzyk, procesów oraz potrzeb Urzędu dokumentacje SZBI oraz BCM zgodne z wymaganiami powołanych wyżej norm i przepisów prawa, obejmujące w szczególności:

* 1. Audyt wstępny:
     1. sprawdzenie i zrozumienie środowiska UM, obejmujący aktualną strukturę organizacyjną i realizowane procesy oraz wymagania prawne funkcjonowania UM,
     2. przegląd aktualnej dokumentacji bezpieczeństwa informacji w UM, w tym polityk, procedur, instrukcji, regulaminów, wytycznych,
     3. inwentaryzację i analizę aktywów - zasobów informacyjnych oraz środków służących do gromadzenia i przetwarzania informacji.
  2. Przeprowadzenie przy udziale przedstawicieli Zamawiającego i udokumentowanie analizy ryzyka, w tym opracowanie i wdrożenie metodyk. Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanej metodyki analizy ryzyka, a Wykonawca zobowiązany jest je uwzględnić. Ponadto Wykonawca zobowiązany jest do przeprowadzenia procesu szacowania ryzyka zgodnie z wybraną i zatwierdzoną przez Zamawiającego metodyką szacowania ryzyka.
  3. Wskazanie obszarów wymagających dostosowania i/lub doskonalenia adekwatnie do przeprowadzonej analizy ryzyka oraz wymagane do wdrożenia zabezpieczenia.
  4. Wykonawca, na podstawie wyników audytów, procesu klasyfikacji informacji oraz szacowania ryzyka, zobowiązany jest zaproponować organizację Systemu Zarządzania Bezpieczeństwem Informacji oraz opracować i przedstawić koncepcję wdrożenia. Koncepcja będzie w szczególności zawierać mapę dokumentów, stanowiącą szczegółowy wykaz dokumentów z zaznaczeniem ich wzajemnych powiązań. Zamawiający zastrzega sobie prawo do wnoszenia uwag do zaproponowanej przez Wykonawcę mapy dokumentów, w tym do rodzaju dokumentów, ich liczby, nazewnictwa oraz zakresu merytorycznego. Uwagi wniesione przez Zamawiającego muszą zostać uwzględnione przez Wykonawcę w koncepcji wdrożenia SZBI.
  5. Na podstawie zatwierdzonej przez Zamawiającego koncepcji Wykonawca przystąpi do opracowania kompletnej dokumentacji SZBI (wszystkich wymaganych przez powołane normy polityk, planów, procedur, instrukcji, metodologii zarządzania ryzykiem itd.) oraz BCM w zakresie systemów informatycznych. Przygotowana dokumentacja powinna uwzględniać procedury i regulaminy obowiązujące w Urzędzie.   
     Wymagane jest odniesienie do wszystkich celów stosowania zabezpieczeń, o których mowa w załączniku A do normy ISO 27001 w postaci mapowania: wymaganie załącznika A -> zabezpieczenie.   
     Opracowane polityki, procedury itd. muszą realnie odnosić się do procesów w UM. Zamawiający oczekuje, że opracowane dokumenty będą napisane zwięźle, językiem zrozumiałym dla osób nie posiadających wysokiego przygotowania z zakresu bezpieczeństwa informacji.   
     Jednocześnie Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanej przez Wykonawcę dokumentacji. Wykonawca jest zobowiązany do uwzględnienia w dokumentacji uwag wniesionych przez Zamawiającego. Wszelkie błędy w przygotowanej dokumentacji świadczące o tym, że dokumentacja została przeniesiona z innej organizacji będą podstawą do odrzucenia dokumentów do poprawki, bez ich dalszej analizy ze strony Zamawiającego.
  6. Przeprowadzenie szkoleń z zakresu opracowanego i wdrożonego w Urzędzie SZBI, w formie szkolenia e-learningowego oraz stacjonarnego (warsztatowego).
     1. Wykonawca zobowiązany jest do przygotowania i dostarczenia utrwalonego co najmniej 60 minutowego szkolenia e-learningowego w formie nagrania audiowizualnego nt. SZBI z przeznaczeniem dla pracowników Zamawiającego. Szkolenie musi być zrealizowane w całości w języku polskim i przedstawione w sposób zrozumiały dla osób nietechnicznych. Nagranie przeznaczone będzie do wielokrotnego odtwarzania bez ograniczeń czasowych i obejmować ma swoim zakresem omówienie co najmniej następujących zasad:
        + bezpieczeństwa przetwarzania informacji, wynikających z PBI,
        + odpowiedzialności za naruszenie zasad SZBI i PBI,
        + zgłaszania i reagowania na incydenty.

Szkolenie e-learningowe musi poprawnie uruchamiać się i płynnie działać na następujących przeglądarkach internetowych w najnowszych wersjach: Microsoft Edge, Mozilla Firefox, Google Chrome, przy czym uruchomienie szkolenia nie powinno wymagać użycia technologii: JAVA, Adobe Flash Player i Microsoft Silverlight.

* + 1. Przeprowadzenie szkolenia na miejscu u Zamawiającego w formie warsztatowej z zakresu SZBI i PBI oraz oceny ryzyka i oceny skutku dla ochrony informacji przetwarzanych w Urzędzie dla pracowników Wydziału Informatyki (ilość osób do szkolenia: 7 osób), Biura Ochrony Danych (ilość osób do szkolenia: 3 osoby) oraz Wydziału Kontroli i Audytu Wewnętrznego (ilość osób do szkolenia: 1 osoba). Szkolenie powinno zawierać materiały szkoleniowe niezbędne do umożliwienia tworzenia w przyszłości kolejnych dokumentów szacowania ryzyka i oceny skutku dla ochrony informacji przetwarzanych w Urzędzie. Czas trwania szkolenia – min. 8 h (2 dni po 4h/dziennie).
    2. Przeprowadzenie szkolenia na miejscu u Zamawiającego dla osób z Zarządu Miasta Opola (max 10 osób). W zakresie wdrożonego SZBI i PBI oraz oceny ryzyka i oceny skutku dla ochrony informacji przetwarzanych w Urzędzie. Czas trwania szkolenia– min. 1,5 h.
  1. Przeprowadzenie przy udziale Zamawiającego audytu wewnętrznego po upływie około 2 miesięcy od wdrożenia SZBI. Celem audytu jest ocena funkcjonowania SZBI. Na podstawie wyników audytu Wykonawca dokona przeglądu dokumentacji SZBI i wprowadzi wszystkie niezbędne korekty/poprawki. Po zakończeniu audytu Wykonawca przygotuje i przekaże w formie elektronicznej oraz papierowej sprawozdanie z przeprowadzonego audytu i naniesie dane do ankiety wskazanej w załączniku nr 6 do regulaminu konkursu.
  2. Udział w audycie zewnętrznym (certyfikującym), który zostanie zlecony przez Zamawiającego w terminie do 60 dni od zakończenia audytu wewnętrznego. Zadaniem Wykonawcy będzie udzielanie wyjaśnień i konsultacji dotyczących wdrożonego SZBI, oraz wprowadzenie ewentualnych zmian lub poprawek w dokumentacji SZBI w przypadku wykazania takiej konieczności.

1. **Termin wykonania zamówienia:**
   1. Zadanie 1.1 - do 30 dni od dnia zawarcia umowy.
   2. Zadanie 1.2, 1.3 i 1.4 - do 60 dni od dnia zawarcia umowy.
   3. Zadanie 1.5 i 1.6 - do 120 dni od dnia zawarcia umowy.
   4. Zadanie 1.7 - do 45 dni od zakończenia zadań od 1.1 do 1.6
   5. Zadanie 1.8 - do czasu zakończenia audytu zewnętrznego (nie dłużej niż 60 dni).
2. **Warunki wynagrodzenia i płatności:**

Wykonawca za realizację zamówienia otrzyma wynagrodzenie podzielone na 4 części, według poniższego podziału.

* 1. Zadanie od nr 1.1 do 1.4 – 25% kwoty umownej,
  2. Zadanie od nr 1.5 do 1.6 – 25% kwoty umownej,
  3. Zadanie nr 1.7 – 25% kwoty umownej,
  4. Zadanie nr 1.8 – 25% kwoty umownej,

1. **Oznaczenie przedmiotu zamówienia wg Wspólnego Słownika Zamówień (CPV):**

Kod i nazwa CPV:

79417000-0 - Usługi doradcze w zakresie bezpieczeństwa.

1. **Inne istotne warunki zamówienia:**
   1. O udzielnie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają łącznie warunki:
      1. W okresie ostatnich trzech lat wykonali usługi wdrożenia systemu zarządzania bezpieczeństwem informacji wg normy PN-EN ISO/IEC 27001 w co najmniej dwóch organizacjach zatrudniających powyżej 300 osób (wg dnia podpisania umowy), w tym w co najmniej jednym urzędzie administracji publicznej.
      2. W okresie ostatnich trzech lat wykonali usługi audytu systemu zarządzania bezpieczeństwem informacji wg normy PN-EN ISO/IEC 27001 w co najmniej trzech organizacjach zatrudniających powyżej 300 osób (wg dnia podpisania umowy), w tym w co najmniej jednym urzędzie administracji publicznej.
      3. W okresie ostatnich trzech lat wykonali usługi szacowania ryzyka w obszarze bezpieczeństwa informacji w co najmniej dwóch organizacjach zatrudniających powyżej 300 osób (wg dnia podpisania umowy), w tym w co najmniej jednym urzędzie administracji publicznej.
      4. W okresie ostatnich trzech lat wykonali usługę opracowania Systemu Zarządzania Ciągłością Działania w obszarze systemów teleinformatycznych w co najmniej jednej organizacji zatrudniającej powyżej 300 osób (wg dnia podpisania umowy),
      5. Dysponują co najmniej 2 osobami, które posiadają aktualny 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 i w okresie ostatnich trzech lat uczestniczyły w co najmniej trzech audytach systemów zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 w organizacjach zatrudniających powyżej 300 osób (wg dnia podpisania umowy), w tym w co najmniej jednym urzędzie administracji publicznej.
      6. Dysponują co najmniej dwoma osobami będącymi specjalistami ds. bezpieczeństwa systemów teleinformatycznych, posiadającymi co najmniej jeden z certyfikatów o których mowa w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu i w okresie trzech ostatnich lat brały czynny udział w co najmniej czterech usługach, których celem było wdrożenie systemu zarządzania bezpieczeństwem informacji w organizacjach zatrudniających powyżej 300 osób, w tym w co najmniej jednym w urzędzie administracji publicznej.
   2. Posiadają ważną polisę OC w zakresie prowadzonej działalności na kwotę ubezpieczenia wysokości min. 500 000 zł.
   3. Zamawiający informuje, że:
      1. nie dopuszcza składania ofert wariantowych lub częściowych,
      2. w toku badania i oceny ofert może żądać od Wykonawcy pisemnych wyjaśnień dotyczących treści złożonej oferty lub innych składanych dokumentów lub oświadczeń. Wykonawca będzie zobowiązanych do przestawienia wyjaśnień w terminie określonym przez Zamawiającego pod rygorem odrzucenia oferty.
      3. wymaga, żeby wszystkie dokumenty i cała korespondencja były w j. polskim,
2. **Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty wraz z podziałem znaczenia kryteriów i sposobu oceny ofert.**
   1. Ocenie zostaną poddane oferty nie podlegające odrzuceniu.
   2. Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującymi kryteriami i ich znaczeniem:

|  |  |  |
| --- | --- | --- |
| **Numer**  **Kryterium** | **Nazwa kryterium** | **Waga podana**  **w procentach** |
| 1 | Cena brutto | 60 |
| 2 | Kryteria jakościowe | 40 |

* 1. Sposób obliczenia wartości punktowej **w kryterium Cena brutto – maksymalnie 60 pkt.**

Ocenie podlega cena całkowita brutto oferty w PLN. Ofercie z najniższą ceną Zamawiający przyzna maksymalną liczbę punktów – 60 pkt. Pozostałym ofertom Zamawiający przyzna punkty obliczone wg wzoru:

Pof– liczba punktów otrzymanych przez daną ofertę w kryterium cena brutto,

Cn – cena najtańszej oferty,

Cb – cena badanej oferty

Obliczenia dokonywane będą przez Zamawiającego z dokładnością do 2 miejsc po przecinku.

* 1. **W kryterium jakościowym** - **maksymalnie 40 pkt.** - wprowadzono podział na dwie grupy:
     1. kryterium podstawowe **(maksymalnie 24 pkt.):** liczba przeprowadzonych wdrożeń systemu zarządzania bezpieczeństwem informacji wg normy PN-EN ISO/IEC 27001 w organizacjach zatrudniających powyżej 300 osób.

Punkty za kryterium podstawowe zostaną przyznane na podstawie oświadczenia Wykonawcy zawartego w „Wykazie wykonanych usług”, o którym pkt. 7.1.2, za ilość wdrożeń w następujący sposób:

* + - * 0 pkt za przeprowadzenie do 2 wdrożeń,
      * 8 pkt za przeprowadzenie od 3 do 5 wdrożeń,
      * 16 pkt za przeprowadzenie od 6 do 15 wdrożeń,
      * 24 pkt za przeprowadzenie 16 i więcej wdrożeń.

Łącznie w ramach tego kryterium Wykonawca może otrzymać maksymalnie 24 pkt.

* + 1. kryterium uzupełniające **(maksymalnie 16 pkt.):** liczba przeprowadzonych audytów zgodności systemu zarządzania bezpieczeństwa informacji, z normą PN-ISO/IEC 27001 w organizacjach zatrudniających powyżej 300 osób.

Punkty za kryterium uzupełniające zostaną przyznane po uzyskaniu co najmniej 8 pkt. w ramach kryterium podstawowego określonego w pkt. 6.4.1, na podstawie oświadczenia Wykonawcy zawartego w „Wykazie wykonanych usług” o którym pkt. 7.1.3, za ilość audytów w następujący sposób:

* + - * 0 pkt za przeprowadzenie do 2 audytów w organizacjach zatrudniających min. 300 osób,
      * 8 pkt za przeprowadzenie co najmniej 3 audytów w organizacjach zatrudniających min. 300 osób,
      * 16 pkt za przeprowadzenie co najmniej 5 audytów w organizacjach zatrudniających min. 300 osób.

Łącznie w ramach tego kryterium Wykonawca może otrzymać maksymalnie 16 pkt.

* 1. Liczba punktów przyznana poszczególnym ofertom zostanie obliczona z dokładnością do dwóch miejsc po przecinku albo z dokładnością wystarczającą do wykazania zróżnicowania ofert niepodlegających odrzuceniu. Za ofertę najkorzystniejszą uznana zostanie oferta, która otrzyma najwyższą liczbę przyznanych punktów.
  2. Jeżeli nie można wybrać oferty najkorzystniejszej z uwagi na to, ze dwie lub więcej ofert otrzyma taką samą sumę punktów, Zamawiający spośród ofert wybiera ofertę z niższą ceną.

1. **Sposób przygotowania oferty:**
   1. Do oferty należy dołączyć:
      1. wypełniony formularz "Formularz ofertowy", który stanowi Załącznik nr 1 do zapytania;
      2. wykaz wykonanych usług wraz dokumentami potwierdzającymi należyte ich wykonanie - wzór stanowi Załącznik nr 5 do zapytania,
      3. wykaz osób wyznaczonych do realizacji niniejszego zamówienia wraz z dokumentami potwierdzającymi posiadane kwalifikacje i doświadczenie - wzór stanowi Załącznik nr 6 do zapytania;
      4. Zamawiający dopuszcza dołączenie poświadczonych za zgodność z oryginałem kopii lub skanów dokumentów, o których mowa w pkt. 7.1.2 i 7.1.3.