Bukowiec, dnia 21.11.2024 r.

ZAPYTANIE OFERTOWE

„Wstępny audyt KRI”

z dnia 21 listopada 2024 r.

Gmina Bukowiec zaprasza do składania ofert na następujące usługi:

- Wstępny audyt bezpieczeństwa informacji, którego kryterium jest *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 (zwanym dalej „Rozporządzeniem KRI”);*

I. Przedmiot zamówienia:

Przedmiotem zamówienia jest:

a) Przeprowadzenie wstępnego audytu bezpieczeństwa zgodnie z § 19 ust. 2 pkt 14 *Rozporządzenia KRI;*
b) Audyt musi być przeprowadzony przez:

- co najmniej dwóch audytorów posiadających uprawnienia wykazane w *Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu,*

Audyt może być zrealizowany w siedzibie zamawiającego lub w formie zdalnej po uzgodnieniu z zamawiającym.

Audyt ma obejmować weryfikację bezpieczeństwa **fizycznego (**sprawdzenie ochrony pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych i zdarzeń takich jak kradzież, nieuprawniony dostęp), **bezpieczeństwa technologicznego** (analiza bezpieczeństwa systemu teleinformatycznego) oraz **bezpieczeństwa organizacyjnego i osobowego (stosowane procedury bezpieczeństwa).**

Audyt musi obejmować weryfikację:

a. systemu zarządzania bezpieczeństwem informacji,
b. zapewnienia aktualizacji regulacji wewnętrznych w zakresie bezpieczeństwa informacji,
c. utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji,
d. przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji,

e. podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia,
f. zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,
g. ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
h. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie,
i. zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
j. ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży,
k. zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych,
l. bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji,
m. zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.

Kryteriami audytów są:

- *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;*
- *Ustawa o Krajowym Systemie Cyberbezpieczeństwa;*
- Norma PN-EN ISO/IEC 27001:2023;
- Norma PN-EN ISO/IEC 27002:2023.

Wykonawca zobowiązany jest do dostarczenia Zamawiającemu:

- raportów z audytów bezpieczeństwa informacji,
- rekomendacji do wdrożenia w celu poprawy cyberbezpieczeństwa Zamawiającego.

Dokumentacja musi obejmować bezpieczeństwo **fizyczne (**ochrona pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych i zdarzeń takich jak kradzież, nieuprawniony dostęp), **bezpieczeństwo technologiczne** (bezpieczeństwo systemu teleinformatycznego) oraz **bezpieczeństwo osobowe i organizacyjne (stosowane procedury bezpieczeństwa).**

Dokumentacja musi obejmować następujące obszary:

a. ustanowienie polityki bezpieczeństwa informacji oraz polityk tematycznych,
b. aktualizacji regulacji wewnętrznych w zakresie bezpieczeństwa informacji,
c. utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji,

d. przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji,
e. podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia,
f. zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,
g. ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
h. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie,
i. zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
j. ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży,
k. zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych,
l. bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji,
m. zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.

Dokumentacja musi uwzględniać wymagania następujących aktów prawnych oraz norm:

- *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;*
- Ustawa o Krajowym Systemie Cyberbezpieczeństwa;
- Norma PN-EN ISO/IEC 27001:2023;
- Norma PN-EN ISO/IEC 27002:2023.

Wykonawca zobowiązany jest do dostarczenia Zamawiającemu:

- kompleksowej dokumentacji systemu zarządzania bezpieczeństwem informacji,
- rekomendacji do wdrożenia w celu poprawy cyberbezpieczeństwa Zamawiającego.

W ramach usługi Zamawiający zapewni wsparcie zespołu wdrożeniowego SZBI Zamawiającego, które odbywać się będzie w formie konsultacji, od poniedziałku do piątku, realizowanych w trakcie wdrożenia, poprzez bezpieczne formy komunikacji, takie jak: rozmowa telefoniczna, poczta e-mail, telekonferencja lub stacjonarnie w siedzibie Zamawiającego.

II. Termin realizacji zadania:

Wykonawca zobowiązuje się wykonać przedmiot umowy w następujących terminach:

- Wykonawca zobowiązuje się do zrealizowania przedmiotu umowy w terminie nie później niż 20 grudnia 2024 r.

III. Kryteria wyboru oferty:

Na kryterium wyboru oferty składa się w 100% cena.

IV. Szczegółowe warunki, jakie musi spełniać przyszły wykonawca

Wymagania względem Wykonawcy

1. W okresie ostatnich 3 lat, zrealizował co najmniej jeden audyt cyberbezpieczeństwa (niewskazany w pkt. b, c, d) o wartości co najmniej 50 000,00 zł brutto w podmiocie realizującym zadania publiczne, potwierdzony referencjami;
2. Zrealizował co najmniej jeden inny audyt bezpieczeństwa informacji z testami penetracyjnymi (niewskazany w pkt. a, c, d) o wartości co najmniej 50 000,00 zł brutto w podmiocie realizującym zadania publiczne, potwierdzony referencjami;
3. Zrealizował co najmniej cztery inne (niewskazane w pkt. a, b, d) audyty cyberbezpieczeństwa o wartości co najmniej 20 000,00 zł brutto w podmiotach realizujących zadania publiczne, potwierdzone referencjami;
4. Wykonał co najmniej 15 innych audytów bezpieczeństwa informacji.

Posiada zespół składający się z co najmniej 3 osób, w tym:

- minimum 2 osobami posiadającymi wiedzę i doświadczenie w zakresie audytowania systemów zarządzania bezpieczeństwem informacji przy spełnieniu wymagań dla audytorów IRCA, CQI lub wymagań równoważnych, tj. określonych na nie niższym poziomie jakości, potwierdzonych zaświadczeniem ukończenia kursu Information Security Management Systems (ISMS) Auditor lub innym równoważnym dokumentem;
- minimum 2 osobami posiadającymi aktualne uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu;
- minimum 1 osobą posiadającą kompetencje w zakresie audytowania systemów zarządzania ciągłością działania przy spełnieniu wymagań dla audytorów wiodących Systemu Zarzadzania Ciągłością Działania zgodnego z normą PN-EN ISO 22301 lub wymagań równoważnych, tj. określonych na nie niższym poziomie jakości, potwierdzone ważnym certyfikatem dla Audytora Wiodącego

Systemu Zarzadzania Ciągłością Działania zgodnego z normą PN-EN ISO 22301 po zdaniu egzaminu lub innym równoważnym dokumentem (zaświadczeniem);

- minimum 2 osobami posiadającymi kompetencje w zakresie audytowania systemów zarządzania jakością przy spełnieniu wymagań dla audytorów wewnętrznych Systemu Zarzadzania Jakością zgodnego z normą PN-EN ISO 9001 lub wymagań równoważnych, tj. określonych na nie niższym poziomie jakości, potwierdzone ważnym certyfikatem dla Audytora Wewnętrznego Systemu Zarzadzania Jakością zgodnego z normą PN-EN ISO 9001 po zdaniu egzaminu lub innym równoważnym dokumentem (zaświadczeniem);
- minimum 2 osobami posiadającymi wiedzę i doświadczenie w zakresie ochrony danych osobowych potwierdzone dyplomem ukończenia studiów podyplomowych w zakresie ochrony danych osobowych oraz posiadającymi co najmniej 8 letnie doświadczenie w pełnieniu funkcji Inspektora Ochrony Danych / Administratora Bezpieczeństwa Informacji;
- minimum 1 osobą posiadającą wiedzę i doświadczenie w zakresie wdrażania systemów zarządzania bezpieczeństwem informacji zgodnie z normą ISO 27001 lub wymagań równoważnych, tj. określonych na nie niższym poziomie jakości, potwierdzone ważnym certyfikatem ukończenia szkolenia w tym zakresie lub innym równoważnym dokumentem (zaświadczeniem) oraz uczestniczącą w projektach wdrożenia systemu zarządzania bezpieczeństwem informacji na podstawie Rozporządzenia KRI w przynajmniej dwóch podmiotach publicznych;
- minimum 1 osobą posiadającą wiedzę i doświadczenie w zakresie ryzyka w ochronie informacji potwierdzoną ważnym certyfikatem ukończenia szkolenia w tym zakresie lub innym równoważnym dokumentem (zaświadczeniem);
- minimum 2 osobami, które uczestniczyły w co najmniej 2 projektach dotyczących zarządzania ryzykiem w bezpieczeństwie informacji, w tym w co najmniej 1 projekcie dotyczącym zarządzania ryzykiem na podstawie normy ISO 27005.
- minimum 1 osobą posiadającą wiedzę w zakresie wymagań *Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* potwierdzoną ważnym certyfikatem ukończenia szkolenia w tym zakresie lub innym równoważnym dokumentem (zaświadczeniem);
- minimum 1 osobą, która przeprowadziła co najmniej 10 szkoleń w zakresie cyberbezpieczeństwa / bezpieczeństwa informacji / ochrony danych dla podmiotów publicznych;
- minimum 1 osobą posiadającą wiedzę w zakresie zarządzania cyberbezpieczeństwem potwierdzoną ważnym certyfikatem ukończenia szkolenia w tym zakresie lub innym równoważnym dokumentem (zaświadczeniem);
- minimum 1 osobą posiadającą wiedzę w zakresie administrowania sieciami teleinformatycznymi, potwierdzoną ważnym certyfikatem ukończenia szkolenia w tym zakresie lub innym równoważnym dokumentem (zaświadczeniem).

- Minimum 1 osobą, która ukończyła wyższe studia techniczne w zakresie cyberbezpieczeństwa oraz uzyskała tytuł inżyniera, potwierdzony dyplomem ukończenia studiów wyższych.
- Minimum 1 osobą, która odbyła specjalistyczne szkolenie w zakresie cyberbezpieczeństwa, na podstawie norm ISO 27001, 22301 i przepisów RODO, potwierdzone certyfikatem ukończenia szkolenia w tym zakresie lub innym równoważnym dokumentem (zaświadczeniem).

W celu spełnienie powyższych warunków udziału w postępowaniu, Wykonawca wraz z ofertą musi dostarczyć:

- Referencje lub inny dokument potwierdzający prawidłowe wykonanie co najmniej jednego audytu cyberbezpieczeństwa (niewskazanego w odpowiedzi na wymóg w ust. II pkt. b, c, d), w ciągu ostatnich 3 lat, o wartości co najmniej 50 000,00 zł brutto w podmiocie realizującym zadania publiczne, potwierdzony referencjami;
- Referencje lub inny dokument potwierdzający prawidłowe wykonanie, co najmniej jednego, innego audytu bezpieczeństwa informacji (niewskazanego w odpowiedzi na wymóg ust. II pkt. a, c, d) o wartości co najmniej 50 000,00 zł brutto, w podmiocie realizującym zadania publiczne;
- Referencje lub inny dokument potwierdzający prawidłowe wykonanie czterech innych audytów cyberbezpieczeństwa (niewskazanych w odpowiedzi na wymóg ust. II pkt. a, b, d) o wartości co najmniej 20 000,00 zł brutto w podmiotach realizujących zadania publiczne;
- Referencje lub inny dokument potwierdzający prawidłowe wykonanie co najmniej 15 innych audytów bezpieczeństwa informacji (niewskazanych w odpowiedzi na wymóg ust. II pkt. a, b, c);
- Referencje lub inny dokument potwierdzający prawidłowe wykonanie co najmniej dwóch projektów dotyczących szacowania ryzyka dla bezpieczeństwa danych w systemach informatycznych, w tym w co najmniej 1 projekcie dotyczącym zarządzania ryzykiem na podstawie normy ISO 27005;
- Referencje lub inny dokument potwierdzający prawidłowe wykonanie co najmniej dwóch projektów polegających na świadczeniu usług w zakresie stworzenia dokumentacji systemu zarządzania bezpieczeństwem informacji dla podmiotów publicznych;
- Co najmniej dwa zaświadczenia ukończenia kursu Information Security Management Systems Auditor (ISMS);
- Co najmniej 2 aktualne certyfikaty wskazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu;
- Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301;
- Co najmniej 2 certyfikaty Audytora Wewnętrznego Systemu Zarządzania Jakością według normy PN-EN ISO 9001;
- Certyfikat ukończenia szkolenia w zakresie wymagań Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

- Certyfikat ukończenie szkolenia w zakresie zarządzania cyberbezpieczeństwem;
- Certyfikat ukończenia szkolenia w zakresie administrowania sieciami teleinformatycznymi;
- Dyplom ukończenia wyższych studiów technicznych w zakresie cyberbezpieczeństwa, potwierdzający uzyskanie tytułu inżyniera;
- Zaświadczenie o odbyciu specjalistycznego szkolenia w zakresie cyberbezpieczeństwa na podstawie norm ISO 27001, 22301 i przepisów RODO;

Sposób przygotowania oferty:

- Ofertę musi być sporządzona w języku polskim
- Wykonawca określi cenę netto i brutto (wraz z podatkiem VAT) dla przedmiotu zamówienia czyli cenę jednostkową, podając ją w złotych polskich, z dokładnością do dwóch miejsc po przecinku.

Badanie ofert:

- W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert.

Oferta zostanie odrzucona:

- jeśli jej treść nie odpowiada wymaganiom określonym w opisie przedmiotu zamówienia oraz wymaganym przez Zamawiającego warunkom realizacji.

Informacje dodatkowe:

- Zamawiający zastrzega sobie prawo do podjęcia negocjacji w zakresie oferowanej ceny.
- W przypadku wybrania oferty najkorzystniejszej, wybrany Wykonawca zostanie poinformowany odrębnym pismem lub telefonicznie.
- Zamawiający zastrzega sobie prawo unieważnienia postępowania o udzielenie zamówienia na każdym etapie jego przeprowadzania bez podania przyczyny.

Postanowienia dotyczące przetwarzania danych osobowych:

Oferent, składając ofertę, wyraża zgodę na przetwarzanie przez Zamawiającego, uczestników postępowania oraz inne uprawnione podmioty danych osobowych w rozumieniu ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. zawartych w ofercie oraz w jej załącznikach.

Zamawiający informuję, że dane osobowe, o których mowa powyżej przetwarzane są w celu wypełnienia prawnie usprawiedliwionego celu, jakim jest w szczególności:

a) przeprowadzenie postępowania o udzielenie zamówienia publicznego;
b) zawarcie i realizacja umowy z wyłonionym w niniejszym postępowaniu Wykonawcą;
c) dokonanie rozliczenia i płatności związanych z realizacją umowy;

d) przeprowadzenia ewentualnych postępowań kontrolnych i/lub audytu przez uprawnione podmioty.

Miejsce i termin złożenia oferty:
Ofertę należy złożyć mailowo na adres: **info@bukowiec.pl**
Termin składania ofert - **do 27 listopada 2024 r., godz. 15:00.**

Osoba uprawniona do kontaktów:
W sprawach technicznych i formalnych:
Grzegorz Radtke, tel. 523309330.

Signature Not Verified

Dokument podpisany przez Adam Licznerski; UG Bukowiec
Data: 2024.11.21 14:46:34 CET
Położenie: Bukowiec; 86-122; kujawsko-pomorskie; Polska