Gmina
Kozienice

Kozienice dn. 27.09.2021

KI.132.17.2021

Zaproszenie do złożenia oferty cenowej

Gmina Kozienice zaprasza do złożenia oferty na usługi audytu dotyczącego bezpieczeństwa informacji, krajowych ram interoperacyjności, RODO, Cyberbezpieczeństwa, przeprowadzenie szkolenia kadry, testów penetracyjnych, aktualizacji dokumentacji i przeprowadzenia analizy ryzyka.

Rodzaj zamówienia: usługa

Kod 72810000-1

Podstawa prawna - art. 2 ust.1 pkt.1 ustawy z dnia 11 września 2019r. Prawo zamówień publicznych (Dz.U. z 2019r. poz. 2019 r z późn. zm.) z uwagi na wartość przedmiotu zamówienia poniżej 130000 zł do niniejszego zamówienia nie mają zastosowania jej przepisy oraz w oparciu o Zarządzenie Nr 259/2016 Burmistrza Gminy Kozienice z dnia 01.12.2016r. w sprawie powołania komisji przetargowej i ustalenia regulaminu udzielania zamówień na dostawy, usługi i roboty budowlane oraz procedury obiegu dokumentów w zakresie udzielania zamówień publicznych w Urzędzie Miejskim w Kozienicach. Postępowanie prowadzone w ramach procedury rozeznania rynku oraz w celu oszacowania wartości zamówienia, w tym kosztów jego realizacji.

Zamawiający:
Gmina Kozienice, ul. Parkowa 5, 26-900 Kozienice
NIP 812-18-28-216, REGON 670223333
tel. 048 611 71 00, faks 048 6142048, strona internetowa: www.kozienice.pl
adres poczty elektronicznej w postępowaniu: piotr.kohut@kozienice.pl
godziny urzędowania Zamawiającego:

- poniedziałek: 8:00 do 17:00
- wtorek-czwartek: 7:30 do 15:30
- piątek: 7:30 do 14:30

I. Określenie przedmiotu zamówienia

Celem jest:

audyt dotyczący bezpieczeństwa informacji, krajowych ram interoperacyjności, RODO, Cyberbezpieczeństwa oraz aktualizacja dokumentacji i przeprowadzenie analizy ryzyka, a także wykonanie testów penetracyjnych i przeprowadzenie szkolenia kadry.

Weryfikacja spełnienia przez systemy teleinformatyczne Zamawiającego wymagań określonych w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 roku 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
Weryfikacja systemu zarządzania bezpieczeństwem informacji i systemu zarządzania usługami IT, wskazanych w Rozporządzeniu, w wymaganiach dla systemów teleinformatycznych.
Analiza systemów IT pod kątem bezpieczeństwa dostępu do danych przechowywanych w formie elektronicznej oraz raport wraz z zaleceniami dotyczącymi procedur ochrony informacji elektronicznej zostanie wykonana w oparciu o:

- Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych z dnia 12 kwietnia 2012 r. (Dz.U. 2017 poz. 2247), zwane dalej Rozporządzeniem

- Normę PN-ISO/IEC 27001 „Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania"
- Normę PN-ISO/IEC 27005 „Technika informatyczna - Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji"
- Normę PN-ISO/IEC 20000-1 „Technika informatyczna - Zarządzanie usługami - Część 1: Specyfikacja"
- Normę PN-ISO/IEC 20000-2 „Technika informatyczna - Zarządzanie usługami – Część 2: Reguły postępowania"
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO),
- Ustawę z 10 maja 2018 r. o ochronie danych osobowych,
- Ustawę z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości,
- Ustawę o informatyzacji działalności podmiotów realizujących zadania publiczne z 17 lutego 2005r. (Dz. U. z 2017 r. poz. 570)
- Ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

Dostarczenie raportu oraz dokumentacji umożliwiającej realizację zaleceń w/w Rozporządzenia, w odniesieniu do wymagań Zamawiającego i określającą dalsze prace związane z wdrożeniem systemu zarządzania bezpieczeństwem informacji

SZCZEGÓŁOWY ZAKRES PRAC

Przeprowadzenie analizy wymagań Zamawiającego w zakresie zarządzania bezpieczeństwem informacji oraz zdefiniowanie zakresu systemu zarządzania bezpieczeństwem informacji podlegającego wdrożeniu, z uwzględnieniem czynników natury organizacyjnej, technicznej i prawnej:

- Opracowanie wykazu przepisów prawnych oraz wymagań z nich wynikających wpływających na system zarządzania bezpieczeństwem informacji Zamawiającego.
- Opis zakresu systemu zarządzania bezpieczeństwem informacji Zamawiającego z uwzględnieniem struktury organizacyjnej Zamawiającego, infrastruktury informatycznej oraz lokalizacji.
- Zdefiniowanie ewentualnych wykluczeń z systemu zarządzania bezpieczeństwem informacji wraz z ich szczegółowym opisem i uzasadnienie

Weryfikacja i aktualizacja polityki systemu zarządzania bezpieczeństwem informacji stanowiącej podstawę dalszych działań związanych z wdrożeniem systemu zarządzania bezpieczeństwem informacji

Polityka systemu zarządzania bezpieczeństwem informacji zawierać będzie w szczególności:

- Określenie podstaw dla systemu zarządzania bezpieczeństwem informacji, w tym podstaw prawnych i normatywnych
- Określenie celu wdrożenia i eksploatacji systemu zarządzania bezpieczeństwem informacji
- Deklarację kadry zarządzającej
- Określenie ogólnej odpowiedzialności w obszarze zarządzania bezpieczeństwem informacji
- Wskazanie ogólnych zasad i metod zarządzania bezpieczeństwem informacji
- Zapewnienie alokacji zasobów niezbędnych do wdrożenia i eksploatacji systemu zarządzania bezpieczeństwem informacji
- Zapewnienie realizacji działań w celu optymalizacji systemu zarządzania bezpieczeństwem informacji.

Weryfikacja procesu zarządzania ryzykiem informacyjnym, przeprowadzenie oceny ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych przez Zamawiającego zgodnie z wytycznymi normy PN-ISO/IEC 27005:2014 oraz przygotowanie planu postępowania z ryzykiem.

- Zdefiniowanie sposobu pomiaru ryzyka w oparciu o rekomendacje normy PN-ISO/IEC 27005
- Zdefiniowanie i opisanie procesu zarządzania ryzykiem
- Przeprowadzenie inwentaryzacji aktywów informacyjnych lub grup aktywów informacyjnych zgodnie z normą PN-ISO/IEC 27005
- Opracowanie katalogu zagrożeń i oszacowanie prawdopodobieństw ich występowania
- Identyfikacja scenariuszy ryzyka i szacowanie ryzyk z uwzględnieniem wyników audytu
- Opracowanie rejestru ryzyk
- Opracowanie planu postępowania z ryzykami. Plan postępowania z ryzykami może uwzględniać, w uzasadnionych przypadkach, wariantowe postępowanie z ryzykami.

Weryfikacja i aktualizacja dokumentacji dotyczącej zabezpieczeń systemu zarządzania bezpieczeństwem informacji.

- Optymalizacja posiadanych przez Zamawiającego dokumentów określających zasady zarządzania bezpieczeństwem informacji, o ile wyniki analizy ryzyka wykażą potrzebę takiej optymalizacji

- Opracowanie dokumentów określających zasady zarządzania bezpieczeństwem informacji, których brak stwierdzono po przeprowadzeniu analizy ryzyka

W weryfikacji mają być wzięte pod uwagę następujące zagadnienia:

- Wymagania w zakresie zabezpieczeń teleinformatycznych
- Zasady bezpiecznego przetwarzania informacji przez pracowników Zamawiającego
- Stosowanie zasady czystego biura i czystego ekranu
- Zabezpieczenie stacji roboczych
- Zasady klasyfikacji informacji i postępowania z informacjami klasyfikowanymi
- Zasady zarządzania dostępem do informacji, w tym nadawania, modyfikacji, odbierania uprawnień oraz przeglądu uprawnień
- Zasady zarządzania dostępem do usług informatycznych, w tym usług sieciowych
- Zarządzanie mechanizmami uwierzytelniającymi, w tym hasłami
- Zasady publikacji informacji w tym: bip, strona internetowa, media społecznościowe
- Zasady wymiany danych z podmiotami zewnętrznymi
- Zasady wewnętrznej wymiany danych
- Zasady postępowania z nośnikami informacji, w tym składowanie i wymiana nośników oraz niszczenie informacji zapisanych na nośnikach
- Zasady wprowadzania zmian w przetwarzaniu informacji, w szczególności z wykorzystaniem systemów informatycznych, z uwzględnieniem testowania bezpieczeństwa wprowadzanych rozwiązań
- Wytyczne w zakresie utrzymania dokumentacji zabezpieczeń i systemów informatycznych
- Zasady zgłaszania podatności w mechanizmach przetwarzających informacje
- Zasady postępowania w przypadku incydentu naruszenia bezpieczeństwa informacji
- Zasady kontroli bezpieczeństwa informacji
- Zasady zarządzania oprogramowaniem
- Zasady zarządzania kopiami zapasowymi
- Zasady zarządzania kopiami archiwalnymi
- Zasady konserwacji i serwisu zabezpieczeń technicznych i systemów informatycznych
- Zasady monitorowania bezpieczeństwa infrastruktury informatycznej
- Zasady przygotowania urządzeń IT do ponownego użycia
- Zasady wycofywania urządzeń IT z użycia
- Zasady bezpiecznego korzystania z urządzeń mobilnych
- Zasady bezpiecznej pracy zdalnej
- Zasady ochrony przed złośliwym oprogramowaniem
- Zasady zarządzania mechanizmami kryptograficznymi
- Zasady monitorowania przepisów prawnych związanych z zabezpieczeniem przetwarzanych informacji oraz wprowadzania zmian wynikających z obowiązków prawnych
- Wytyczne w zakresie ochrony fizycznej i technicznej
- Wytyczne w zakresie monitorowania przepisów prawnych związanych z ochroną informacji
- Wytyczne w zakresie bezpiecznej współpracy z podmiotami zewnętrznymi
- Wytyczne w zakresie bezpiecznego świadczenia usług związanych z przetwarzaniem informacji
- Wytyczne w zakresie bezpieczeństwa osobowego w procesach rekrutacji i zarządzania personelem
- Dokumenty w zakresie ciągłości działania
    - Strategia ciągłości przetwarzania informacji
    - Plan ciągłości działania dla sytuacji uniemożliwienia przetwarzania informacji
    - Zasady testowania planu ciągłości działania

Audyt bezpieczeństwa informacji obejmujący:

Audyt zarządzania bezpieczeństwem danych osobowych, którego celem jest weryfikacja realizacji przez Zamawiającego czynności wymaganych w związku z przetwarzaniem danych osobowych zgodnie z RODO. W skład tego audytu wchodzą:

- Analiza posiadanej przez Zamawiającego dokumentacji związanej z przetwarzaniem danych osobowych
- Weryfikacja realizacji przez Administratora wymaganych czynności
- Zbadanie przesłanek legalności przetwarzania danych osobowych i wrażliwych,
- Weryfikacja celu, zakresu przetwarzania danych oraz adekwatności do celu przetwarzania.

- Weryfikacja procesów przetwarzania danych osobowych oraz określenie konieczności prowadzenia rejestru przetwarzania.
- Analiza fizycznych i logicznych zabezpieczeń infrastruktury informatycznej,
- Weryfikacja poziomu zabezpieczeń procesów danych osobowych przetwarzanych Weryfikacja poziomu wiedzy i świadomości pracowników w zakresie ochrony danych osobowych,

Weryfikacja zawartych umów pod kątem powierzenia przetwarzania danych osobowych

Audyt socjotechniczny, którego celem jest weryfikacja zagrożeń spowodowanych czynnikiem ludzkim. W ramach tego audytu przeprowadzone zostaną następujące testy:

- Próba uzyskania dostępu do komputera;
- Próba uzyskania dostępu do informacji;
- Symulacja umieszczenia szkodliwego oprogramowania na komputerze użytkownika;
- Sprawdzenie „odporności" użytkowników na ataki socjotechniczne z wykorzystaniem takich narzędzi jak: telefon, poczta elektroniczna, przenośna pamięć masowa
- Sprawdzenie sposobu przechowywania haseł przez użytkowników,
- Weryfikacja ochrony powierzonego sprzętu i dokumentacji,
- W szczególności sprawdzenie scenariuszy socjotechnicznych opartych o wysłanie fałszywego maila imitującego wiadomość służbową lub wykonywanie fałszywego telefonu

Audyt fizyczny i środowiskowy, którego celem jest weryfikacja skutecznej ochrony fizycznej i środowiskowej zasobów, w skład tego audytu wchodzi:

- Weryfikacja granic obszaru bezpiecznego
- Weryfikacja zabezpieczeń wejścia/wyjścia
- Weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń
- Weryfikacja bezpieczeństwa okablowania strukturalnego
- Weryfikacja systemów chłodzenia
- Weryfikacja systemów alarmowych

Audyt teleinformatyczny, którego celem jest wykrycie potencjalnych zagrożeń związanych z utratą informacji w systemach informatycznych, w zakresie:

- Weryfikacja i analiza bezpieczeństwa dostępu do wewnętrznej infrastruktury sieciowej IT
- Weryfikacja i analiza jakościowa odporności infrastruktury IT na bezautoryzacyjne rozpoznanie jego składowych, w tym weryfikacja podatności serwisów DNS
- Weryfikacja systemów oraz protokołów zarządzania i monitorowania infrastruktury IT
- Weryfikacja jakościowa ochrony przed oprogramowaniem szkodliwym poprzez próby propagacji testowego oprogramowania szkodliwego. (zarówno z zewnątrz jak i od wewnątrz infrastruktury IT)
- Weryfikacja środków technicznych kontroli dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania
- Weryfikacja i analiza danych przetwarzanych przez systemy logowania
- Weryfikacja podatności logicznych środków kontroli dostępu wewnątrz Infrastruktury IT
- Weryfikacja poufności i integralności przetwarzania danych w systemach bazodanowych, w szczególności danych osobowych
- Weryfikacja identyfikacji oraz autentykacji stosowanych w mechanizmach autoryzacji dostępu do zasobów IT
- Weryfikacja podatności systemów i sieci na ataki takie jak sniffing, spoofing, man-in-the-middle
- Weryfikacja na podstawie otwartości portów, podatności związanych z autoryzacją dostępu zdalnego do zasobów IT i ocena związanych z tym ryzyk
- Weryfikacja bezautoryzacyjnego dostępu do informacji o rodzaju i wersji wykorzystywanego oprogramowania systemowego i usługowego
- Rozpoznanie i ocena mechanizmów zarządzania aktualizacjami - w tym obecność systemów automatyzujących propagację poprawek bezpieczeństwa
- Weryfikacja podatności na bezautoryzacyjne połączenia systemów VoIP
- Weryfikacja podatności hostów na ataki w warstwie systemowej (przy wykorzystaniu exploitów)
- Weryfikacja podatności hostów na możliwość uzyskania nieautoryzowanego dostępu do zasobów plikowych
- Weryfikacja poufności przesyłu danych przetwarzanych na udostępnionych zasobach plikowych
- Weryfikacja podatności ustawień hostów na możliwość uzyskania nieautoryzowanego zdalnego dostępu do kontroli treści przesyłanych przez przeglądarki www
- Weryfikacja bezautoryzacyjnej dostępności do danych o czasie pracy, krytycznych systemów

- Weryfikacja obecności domyślnych kont użytkowników oraz haseł
- Weryfikacja obecności podatnych algorytmów szyfrowania
- Weryfikacja podatności systemów i aplikacji www w wewnętrznej infrastrukturze IT
- Weryfikacja poufności przesyłania danych do wydruku
- Analiza i ocena dodatkowych systemów bezpieczeństwa tj. dodatkowego oprogramowania antywirusowego, oprogramowania weryfikującego integralność systemów i gwarantującego audytowalność infrastruktury IT
- Weryfikacja podatności systemu sieci wewnętrznej na zakłócenie/zablokowanie dostępności do usług i określenie zasięgu oraz zlokalizowanie fizycznego źródła ataku

Przeprowadzenie testów penetracyjnych przeprowadzonych ze stacji roboczej podłączonej do systemu informatycznego z zewnątrz (testy black box) mających na celu zidentyfikowanie jego podatności na włamanie oraz kompromitacje, w zakresie:

Zebranie dostępnych wiadomości o obiekcie metodą pasywną

- Wykorzystanie baz danych i narzędzi on-line: whois, dns, robtex,etc.
- Wyszukiwanie informacji o ostrzeżeniach błędach
- Wyszukiwanie informacji o dostępnych zasobach i plikach

Przeskanowanie wszystkich portów i dostępnych usług na testowanych adresach systemu:

- Identyfikacja aktywnych hostów i otwartych portów
- Podjęcie próby identyfikacji dostępnych usług i ich wersji (weryfikacja wyników skanowania, co najmniej dwoma innymi jeszcze metodami)

Próba identyfikacji testowanego systemu i jego struktury

- Próba określenia typu i wersji systemu operacyjnego
- Analiza informacji zawartych w banerach usług

Próba wykrycia luk i podatności konfiguracyjnych

- Analiza metadanych plików
- Próba enumeracji zasobów danych
- Próba przeprowadzenia ataku słownikowego na hasła użytkowników
- Próba ujawnienia wycieków danych (obecność popularnych plików, analiza informacje o błędach, niewłaściwe nazewnictwo zasobów, wycieki kodu aplikacji)
- Próby wywołania błędów aplikacji (manipulacja przesyłanymi danymi, w tym:)
- Przesyłanie niepoprawnych danych
- Przesyłanie nadmiarowych danych

Praktyczne sprawdzenie wykrytych podatności :

- Próba exploitacji z użyciem bazy posiadanych exploitów
- Próba przeprowadzenia ataku DOS
- Weryfikacja nieautoryzowanego dostępu do testowanego systemu
- Weryfikacja informacji wrażliwych, uzyskanych w odpowiedziach systemu
- Weryfikacja reakcji zabezpieczeń testowanego systemu, na przeprowadzane próby ataku
-

Analiza bezpieczeństwa systemu poczty elektronicznej będący szczególnym przypadkiem audytu teleinformatycznego i rozszerzający zakres audytu teleinformatycznego o:

- Weryfikację oprogramowania AV poczty elektronicznej na rozsyłanie zagrożeń zawierających w treści zagrożenia, przesyłanych z wewnątrz i zewnątrz infrastruktury IT
- Badanie podatności systemu poczty na próby bezautoryzacyjnego dostępu do skrzynek poczty elektronicznej pracowników
- Badanie podatności systemu dostępu przez www do poczty elektronicznej
- Badanie podatności systemu na próby bezautoryzacyjnego rozsyłania poczty elektronicznej

Analiza bezpieczeństwa usługi katalogowej Active Directory będący szczególnym przypadkiem audytu teleinformatycznego i rozszerzający zakres audytu teleinformatycznego o:

- Weryfikację bezpieczeństwa transmisji danych pomiędzy serwerem a stacjami roboczymi

- Weryfikację reakcji i czasu reakcji na atak account lockout w domenie
- Weryfikację bezpieczeństwa poufności przesyłanych danych potrzebnych do autoryzacji, z urządzeń zintegrowanych z AD
- Weryfikację bezpieczeństwa poufności instrukcji GPO pod kątem ujawniania krytycznych informacji o systemach i wycieku danych

Raport z audytu, który zawiera:

- Cel i zakres audytu
- Opis źródeł informacji wykorzystanych podczas przeprowadzania audytu
- Dowody na obecność wykrytych podatności oraz popierające zawarte w raporcie analizy i stwierdzenia
- Ocenę zabezpieczeń i rekomendowane działania korekcyjne

Szkolenia dla pracowników Zamawiającego wraz z potwierdzeniem imiennym odbytego szkolenia

Szkolenie skierowane do pracowników Zamawiającego obejmujące:

- Omówienie podstawowych zasad bezpieczeństwa informacji i wypełniania procedur bezpieczeństwa informacji
- Omówienie obowiązku informacyjnego w administracji ćwiczenia praktyczne
- Zagrożenia związane z przetwarzaniem informacji
- Odpowiedzialność za naruszenie zasad bezpieczeństwa informacji;
- Zasady zgłaszania i procedury reagowania na incydenty.

Wykonawca przekaże Zamawiającemu prezentacje z przeprowadzonych szkoleń, a także wystawi imienne potwierdzenia odbytego szkolenia.

II. Termin wykonania zamówienia: 45 dni od dnia podpisania umowy.

1. Wykonawca, w terminie do 45 dni od dnia podpisania umowy dostarczy Zamawiającemu przedmiot zamówienia.
2. W przypadku nie dotrzymania terminów, o których mowa powyżej Zamawiający zastrzega sobie prawo rozwiązania umowy z winy Wykonawcy naliczenie kar umownych.

III. Wymagania w stosunku do Wykonawcy

W postępowaniu mogą wziąć udział Wykonawca, który:

1. Zrealizował przynajmniej 30 audytów bezpieczeństwa informacji w instytucjach publicznych w ostatnich 2 latach, licząc do terminu składania oferty.
   Wykonawca, który złoży ofertę zobowiązany będzie jest do załączenie w ofercie wykazu usług i referencji potwierdzających należyte wykonanie tych usług.
2. Dysponuje w ramach umowy o pracę osobami zdolnymi zrealizować zamówienie:
   a. Trzech audytorów z wykształceniem wyższym, w tym jeden z wyższym technicznym informatycznym,
   b. Trzech audytorów z wykształceniem wyższym z ochrony danych osobowych.
   c. Dwóch audytorów wiodących ISO/IEC 27001 ze zdanym egzaminem IRCA,
   d. Jeden audytor wiodący ISO 22301 ze zdanym egzaminem IRCA,
   e. Jeden audytor wewnętrzny ISO 27001,
   f. Audytor posiadający zaświadczenie Certified Information Systems Security Officer (CISSO) lub równoważny,
   g. Audytor posiadający certyfikat Microsoft Certified Solutions Expert (MCSE) lub równoważny,
3. Prowadzi działalność w zakresie, którego dotyczy przedmiot zamówienia przez okres co najmniej 7 lat przed dniem złożenia oferty.
4. Posiada polisę ubezpieczeniową o wartości co najmniej 150 000 zł.
5. Posiada aktualne Zaświadczenia o niezaleganiu ze składkami ZUS i podatkiem w US.
6. Nie jest dopuszczalne wykonywanie audytu przez podwykonawców.

Wykonawca, który złoży najkorzystniejszą ofertę zobowiązany będzie do przedstawienia wymaganych certyfikatów i dokumentów.

IV. Przygotowanie oferty

1. Ofertę należy sporządzić zgodnie z formularzem oferty stanowiącym załącznik nr 1 do niniejszego zaproszenia.

2. Oferta musi być sporządzona w formie pisemnej i być podpisana przez osobę uprawnioną.
3. W przypadku, gdy ofertę podpisuje osoba inna niż wynika to z dokumentów rejestrowych, do oferty należy dołączyć pełnomocnictwo, zgodne z wymaganiami Kodeksu cywilnego upoważniające do wykonania tej czynności.
4. Do oferty należy dołączyć dokumenty i oświadczenia, o których mowa w pkt. III. 3.
5. Wszystkie załączniki do oferty, stanowiące oświadczenia powinny być podpisane przez upoważnionego przedstawiciela. Zakres reprezentacji przedsiębiorcy musi wynikać z dokumentów przedstawionych przez Wykonawcę.
6. Kserokopie dokumentów muszą być poświadczone za zgodność z oryginałem przez Wykonawcę.
7. Koszty sporządzenia i złożenia oferty ponosi Wykonawca.
8. Wykonawca może złożyć w prowadzonym postępowaniu wyłącznie jedną ofertę obejmującą całość usług, o których mowa w pkt. I zaproszenia.

V. Opis sposobu obliczenia ceny oferty

1. Cenę oferty za wykonanie przedmiotu zamówienia Wykonawca wskaże w Formularzu oferty (zał. nr 1 do zaproszenia). Wykonawca zobowiązany jest do właściwego i szczegółowego wypełnienia druku oferty i załączników do oferty. Dane zawarte w ofercie są podstawą weryfikacji Wykonawcy.
2. Cena oferty ma być wyrażona w PLN jako cena brutto i winna obejmować wszystkie koszty i opłaty, jakie powstaną w związku z wykonaniem zamówienia, w tym w szczególności: materiały i czynności uznane przez Wykonawcę jako niezbędne do prawidłowego wykonania dostawy, opłaty niewymienione, które mogą wystąpić przy realizacji przedmiotu zamówienia, wszelkie podatki i opłaty, w tym należny podatek VAT, ewentualne opusty oraz inne składniki cenotwórcze.
3. Jeżeli ofertę złoży osoba fizyczna nieprowadząca działalności gospodarczej, w cenę oferty należy wyliczyć składki na ubezpieczenie społeczne i zdrowotne oraz zaliczkę na podatek dochodowy, które to Zamawiający, zgodnie z obowiązującymi przepisami, zobowiązany byłby naliczyć i odprowadzić.
4. Cenę za wykonanie zamówienia należy wyliczyć wg. kalkulacji własnej. W cenie ofertowej należy uwzględnić wszelkie koszty, jakie Wykonawca przewiduje ponieść na wykonanie dostawy.
5. Zamawiający wyklucza możliwość roszczeń Wykonawcy z tytułu błędnego skalkulowania ceny lub pominięcia elementów niezbędnych do wykonania zamówienia.

VI. Miejsce i termin składania i otwarcia ofert

1. Ofertę cenową sporządzoną na Formularzu oferty (zał. nr 1) wraz z załącznikami należy złożyć w **siedzibie Urzędu Miejskiego w Kozienicach, ul. Parkowa 5, 26-900 Kozienice, w pok. Nr 111- Sekretariat, w terminie do dnia 01.10.2021 r. do godz. 09:00.**
2. Ofertę cenową należy złożyć w zamkniętej kopercie opatrzonej napisem: **„Oferta na usługi audytu dotyczącego bezpieczeństwa informacji, krajowych ram interoperacyjności, RODO, Cyberbezpieczeństwa, Szkolenia, testów penetracyjnych, aktualizacji dokumentacji i przeprowadzenia analizy ryzyka."** z dopiskiem **„Nie otwierać przed dniem 01.10.2021 r. przed godz. 09: 00"** Otwarcie ofert nie ma charakteru publicznego.
3. Oferty złożone po terminie wyznaczonym do składania ofert nie będą rozpatrywane. Oferty pozostaną u Zamawiającego bez otwierania.
4. Wykonawca może przed upływem terminu na składanie ofert zmienić lub wycofać swoją ofertę, składając pisemny wniosek do Zamawiającego.

VII. Kryteria oceny ofert i ocena ofert

1. Zamawiający dokona oceny ofert ważnych, spełniających wymagania określone w zaproszeniu, na podstawie kryterium:

1.1. Cena-100%.

2. Ocena ofert w kryterium **„Cena"** zostanie dokonana wg następujących zasad:

Ocenie zostanie poddana cena brutto. Liczba punktów w kryterium „cena" (C) zostanie obliczona na podstawie poniższego wzoru:

$$C = \frac{Cmin}{Co} \times 100\%$$

gdzie:

C	liczba punktów za kryterium „cena"
Cmin	najniższa cena oferty brutto z ocenianych ofert (zł)
Co	cena oferty brutto określona w badanej ofercie (zł)

1. Najwyższa liczba punktów wyznaczy najkorzystniejszą ofertę.

VIII. Inne postanowienia

1. W toku rozpatrywania ofert cenowych Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonej oferty cenowej oraz prowadzić dodatkowe negocjacje z Wykonawcami, którzy odpowiedzieli na zapytanie ofertowe.
2. Zamawiający drogą elektroniczną powiadomi o wyborze Wykonawcę, którego oferta cenowa zostanie wybrana.
3. Zamawiający może unieważnić postępowanie bez podania przyczyny. Z tego tytułu, w stosunku do Zamawiającego, nie będą przysługiwać Wykonawcy żadne roszczenia.
4. Forma udzielenia zamówienia - umowa.
5. Istotne postanowienia i warunki, które zostaną wprowadzone do treści umowy zawiera projekt umowy - zał. nr 2 do niniejszego zaproszenia. Zamawiający zawrze umowę z wybranym Wykonawcą wg wzoru zawartego w załączniku nr 2.
6. Wymagany okres gwarancji na przedmiot umowy wynosi min. 12 miesięcy i będzie liczony od daty odbioru przedmiotu zamówienia.
7. Pytania do postępowania można zadawać drogą elektroniczną lub pisemną w terminie do dnia 30.09.2021 r. do godz. 14:00 /liczy się data i godz. wpływu do Zamawiającego/. Zamawiający udzieli odpowiedzi na pytania pocztą elektroniczną w dniu następnym.
8. Na zapytania złożone po dniu 30.09.2021 r. Zamawiający nie będzie udzielał odpowiedzi.
9. **Zamawiający informuje, że odmowa podpisania umowy przez Wykonawcę, którego oferta została wybrana w niniejszym postępowaniu, z jego winy, może skutkować, że w kolejnych postępowaniach oferta takiego Wykonawcy nie będzie rozpatrywana (będzie podlegać odrzuceniu).**

IX. Informacja dotycząca ochrony danych osobowych

Zgodnie z art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) - dalej RODO Gmina Kozienice informuje, iż:

1. Administratorem Pani/Pana danych osobowych : Burmistrz Gminy Kozienice
2. Siedziba Administratora: Urząd Miejski, ul. Parkowa 5, 26-900 Kozienice
3. Kontakt z Inspektorem Ochrony Danych- iod@kozienice.pl
4. Pani/Pana dane osobowe przetwarzane będą w celu realizacji zamówienia - na podstawie Art. 6 ust. 1 lit. b i c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego oraz w celu archiwizacji.
5. Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty uczestniczące w realizacji umowy oraz wszyscy którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy z dnia 29 stycznia 2004r. - Prawo zamówień publicznych (tj. Dz. U. z 2018r. poz. 1986) a także podmioty przetwarzające dane na podstawie zawartych umów.
6. Pani/Pana dane osobowe przechowywane będą przez okres obowiązywania umowy, a następnie 10 lat po zakończeniu okresu obowiązywania umowy. Okres ten dotyczy również Wykonawców, którzy złożyli oferty i nie zostały one uznane jako najkorzystniejsze (nie zawarto z tymi Wykonawcami umowy/zlecenia).
7. obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
8. Posiada Pani/Pan prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania.
9. Ma Pani/Pan prawo wniesienia skargi do organu nadzorczego .
10. Podanie danych osobowych jest dobrowolne, jednakże odmowa podania danych może skutkować odmową

zawarcia umowy.

11. nie przysługuje Pani/Panu:

- w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
- na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

Załączniki:

1. Formularz oferty - zał. nr 1.
2. Wzór umowy-zał. nr 2.

BURMISTRZ GMINY KOZIENICE
mgr Piotr Kozłowski

Sprawę prowadzi:
- Pan/~~Pani~~ Piotr Kohut. e-mail: piotr.kohut@kozienice.pl
Wydział Kadr, obsługi Rady i Informatyzacji Urzędu Miejskiego w Kozienicach
tel. 48 6117193

ADWOKAT
Andrzej Kowalik

Załącznik nr 1 – Wzór Formularza Oferty

Pieczęć Wykonawcy/wców	..... **Miejscowość i data**

Nr tel/fax .....

e-mail: .....

Województwo:.....

Adres do korespondencji: .....

.....

NIP .....**Regon**.....**KRS/CEiDG**.....
(podać wszystkie dane)

GMINA KOZIENICE
ul. Parkowa 5
26-900 Kozienice

OFERTA CENOWA

W odpowiedzi na zaproszenie do złożenia oferty na na usługi audytu dotyczącego bezpieczeństwa informacji, krajowych ram interoperacyjności, RODO, Cyberbezpieczeństwa, Szkolenia, testów penetracyjnych, aktualizacji dokumentacji i przeprowadzenia analizy ryzyka.

Ja/My niżej Podpisany/podpisani

.....

(dane osoby upoważnionej do podpisania oferty)

działając w imieniu i na rzecz Wykonawcy/wykonawców[1]:

Lp.	Nazwa (y) Wykonawcy (ów)	Adres (y) Wykonawcy (ów)

uwzględniając zakres, warunki i wymagania zawarte w zaproszeniu, składamy niniejszą ofertę:

1. Oferujemy wykonanie zamówienia w zakresie określonym w zaproszeniu, zgodnie z opisem przedmiotu zamówienia :

   za cenę brutto ..... PLN, **słownie:** .....

   .....

2. Zamówienie wykonamy w terminie: 45 **dni** od dnia podpisania umowy.

[1] Podać nazwę Wykonawcy, a w przypadku wykonawców występujących wspólnie należy podać nazwy i adresy wszystkich wykonawców (wszystkich wspólników spółki cywilnej lub członków konsorcjum)

3. Oświadczamy, że na wykonaną usługę udzielamy 12 **miesięcznej gwarancji jakości i rękojmi,** liczonej od daty końcowego odbioru przedmiotu niniejszego postępowania.

4. Oświadczamy, że:
   1) Powyższa cena uwzględnia wszystkie koszty, jakie ponosi zamawiający w przypadku wyboru niniejszej oferty,
   2) Zapoznaliśmy się z otrzymanymi dokumentami, w pełni je akceptujemy i nie wnosimy do nich zastrzeżeń oraz przyjmujemy warunki w nich zawarte,
   3) Spełniamy warunki udziału w postępowaniu o których mowa w pkt. III.1-6 zaproszenia do złożenia oferty, tj.:
      - posiadamy wiedzę i doświadczenie niezbędne do wykonania niniejszego zamówienia,
      - dysponujemy osobami posiadającymi odpowiednie uprawnienia zawodowe do wykonania zamówienia,
      - znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie niniejszego zamówienia,
   4) Nie podlegamy wykluczeniu z postępowania w okolicznościach, o których mowa w art. 108 ust. 1 ustawy Prawo zamówień publicznych.
   5) Wobec mnie/mojej Firmy nie toczy się żadne postępowanie likwidacyjne lub upadłościowe i nie figuruję/żadna z osób reprezentujących moją Firmę nie figuruje w Krajowym Rejestrze Karnym,
   6) Zamówienie wykonamy siłami własnymi/ przy pomocy następujących podwykonawców* (*niewłaściwe skreślić) .....
      .....
      którym powierzymy wykonanie następujących części zamówienia .....
      .....

5. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[1)] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu. (W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO - *treść oświadczenia wykonawcy nie dotyczy).*

6. W przypadku przyznania nam zamówienia zobowiązujemy się do zawarcia umowy na warunkach zawartych w projekcie umowy, w miejscu i terminie wyznaczonym przez Zamawiającego.

7. Oświadczam, że pozostaje związany ofertą na okres 30 dni, licząc od dnia wyznaczonego do złożenia oferty.

8. Załącznikami do niniejszej oferty są:

   1) .....

   2) .....

   3).....

   4) .....

   5)..... .....

(podpis osoby/osób uprawnionych do reprezentowania Wykonawcy/Wykonawców)

Kl.132.17.2021

UMOWA

zawarta w Kozienicach
dnia .10.2021r.

pomiędzy:

Gminą Kozienice z siedzibą w Kozienicach (26-900), ul. Parkowa 5 NIP: 8121828216, REGON: 670223333 zwaną dalej **Zamawiającym**, reprezentowaną przez:
- Pana Piotra Kozłowskiego - Burmistrza Gminy Kozienice przy kontrasygnacie Pani Moniki Makulec-Soboty - Skarbnika Gminy Kozienice

a:

.....
NIP: ....., REGON: ....., KRS/CEIDG .....
zwaną dalej **Wykonawcą.** reprezentowaną przez:

.....

o następującej treści:

PRZEDMIOT UMOWY

§ 1

Przedmiotem umowy jest usługa audytu dotyczącego bezpieczeństwa informacji, krajowych ram interoperacyjności, RODO, Cyberbezpieczeństwa, szkolenia kadry, testów penetracyjnych, aktualizacji dokumentacji i przeprowadzenia analizy ryzyka. Szczegółowo określony w zapytaniu ofertowym (sygn. akt. Kl.132.17.2021 z dnia 27 września 2021 r.) stanowiącym *Załącznik Nr 1* do niniejszej umowy.

WYNAGRODZENIE

§ 2

1. Za wykonanie przedmiotu umowy określonego w § 1 **Zamawiający** zobowiązuje się zapłacić **Wykonawcy** wynagrodzenie w łącznej wysokości ..... zł **brutto** (słownie: ..... złotych ..... groszy).
2. Wynagrodzenie, o którym mowa w ust.1 jest stałe i obejmuje całość wynagrodzenia należnego **Wykonawcy** z tytułu niniejszej umowy, nie może ulegać zmianom w trakcie realizacji umowy oraz obejmuje wszelkie koszty i wydatki **Wykonawcy** związane z realizacją przedmiotu umowy, z uwzględnieniem podatku od towarów i usług, innych opłat oraz ewentualnych upustów i rabatów.
3. Wynagrodzenie zostanie wypłacone przelewem na rachunek bankowy wskazany na prawidłowo wystawionej fakturze/rachunku VAT, dostarczonego do siedziby **Zamawiającego**.
4. Wynagrodzenie będzie płatne w terminie 14 dni od dnia wpłynięcia na sekretariat Urzędu Miejskiego w Kozienicach (siedziby **Zamawiającego**) prawidłowo wystawionej faktury/rachunku VAT po podpisaniu przez obie strony umowy bezusterkowego protokołu odbioru przedmiotu umowy stanowiącego *Załącznik Nr 2* do niniejszej umowy, który dostarcza **Wykonawca**.

KARY UMOWNE

§ 3

1. W przypadku nie dostarczenia przedmiotu umowy w terminie określonym w zapytaniu ofertowym (sygn. akt. Kl.132.17.2021 z dnia 27 września 2021 r.) stanowiącym *Załącznik Nr 1* do niniejszej umowy **Wykonawca** zapłaci karę umowną w wysokości 0,5% całkowitej wartości wynagrodzenia brutto określonego w § 2 ust. 1 niniejszej umowy za każdy dzień opóźnienia.

2. W przypadku odstąpienia przez **Zamawiającego** od umowy z przyczyn zależnych od **Wykonawcy, Wykonawca** zapłaci karę umowną w wysokości - 30% wartości wynagrodzenia całkowitego brutto za wykonanie przedmiotu umowy, określonego w § 2 ust. 1 niniejszej umowy.

3. **Zamawiający** zastrzega sobie prawo potrącania kar umownych z bieżącego wynagrodzenia **Wykonawcy i na co Wykonawca wyraża zgodę.**

4. **Zamawiający** ma prawo dochodzić odszkodowania przewyższającego wysokość kary umownej - na zasadach Kodeksu Cywilnego - do wysokości rzeczywiście poniesionej szkody.

5. W przypadku opóźnienia w zapłacie wynagrodzenia wynikającego z treści niniejszej umowy **Zamawiający** zobowiązuje się do zapłaty **Wykonawcy** odsetek ustawowych za opóźnienie.

6. Łączna maksymalna wysokość kar umownych, których mogą dochodzić strony wynosi 40% wartości brutto umowy określonej w § 2 ust 1 umowy.

GWARANCJA

§ 4

1. **Wykonawca** udziela **Zamawiającemu** gwarancji jakości na dostarczony i wykonany przedmiot umowy na okres 12 miesięcy, a termin gwarancji liczy się od daty bezusterkowego odbioru przedmiotu umowy.
2. Wszelkie usterki **Wykonawca** usunie w ciągu 14 dni od momentu zgłoszenia.
3. Wykonawca zapewnia zgodność przeprowadzonego audytu zgodnie z normami ujętymi w specyfikacji tego postępowaniu i w tym celu podejmuje wszelkie możliwe starania, aby dostarczane przez niego usługi pozbawione było błędów, które utrudniają lub uniemożliwiają jego efektywne wykorzystywanie przez Zamawiającego.

POSTANOWIENIA KOŃCOWE

§ 5

1. Umowa wiąże strony z dniem jej podpisania przez **Wykonawcę** i **Zamawiającego** i zostaje zawarta na czas spełnienia wszystkich świadczeń w niej zawartych.

2. **Wykonawca** zobowiązany jest do odesłania podpisanej umowy w dniu podpisania na adres mailowy urzad@kozienice.pl oraz na adres korespondencyjny **Zamawiającego** (Urząd Miejski w Kozienicach, ul. Parkowa 5, 26-900 Kozienice).

3. W sprawach nieuregulowanych umową stosuje się przepisy Kodeksu Cywilnego i Ustawy o prawie autorskim i prawach pokrewnych.

4. **Wykonawca** i **Zamawiający** oświadczają, ze dołożą wszelkich starań, aby ewentualne spory, jakie mogą powstać przy realizacji postanowień niniejszej umowy były rozwiązywane polubownie poprzez bezpośrednie negocjacje.

5. Ewentualne spory, które mogą zaistnieć między stronami na tle wykonywania niniejszej umowy, których nie uda się rozwiązać polubownie w bezpośrednich negocjacjach, będą rozstrzygane przez sąd wg właściwości miejscowej **Zamawiającego.**

6. Zmiany i uzupełnienia umowy wymagają formy pisemnej pod rygorem nieważności.

7. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, jeden dla **Wykonawcy**, jeden dla **Zamawiającego**.

WYKONAWCA **ZAMAWIAJĄCY**

ADWOKAT
Andrzej Kowalik