

Gmina Piątnica
ul. Stwiskowska 53
18-421 Piątnica Poduchowna
SO.2151.4.2016

ZAPROSZENIE
do złożenia propozycji cenowej
Gmina Piątnica z siedzibą w Piątnicy Poduchownej,
(pełna nazwa zamawiającego)

ul. Stawiskowska 53, 18-421 Piątnica Poduchowna zaprasza do złożenia propozycji cenowej na:

audyt w zakresie bezpieczeństwa informacji w Urzędzie Gminy Piątnica, opracowanie: Polityki Bezpieczeństwa, Instrukcji Zarządzania Systemem Informatycznym, wskazań w zakresie wdrożenia ogólnego rozporządzenia o ochronie danych oraz szkolenie pracowników z zakresu bezpieczeństwa informacji i ochrony danych osobowych

1. Opis sposobu przygotowania propozycji cenowej:

- 1.1. należy ją złożyć w zamkniętej kopercie,
- 1.2. na kopercie należy umieścić nazwę i adres zamawiającego, nazwę i adres wykonawcy oraz napis: "Propozycja cenowa na audyt w zakresie bezpieczeństwa informacji",
- 1.3. ceny w niej podane mają być wyrażone cyfrowo i słownie,
- 1.4. ma być napisana w języku polskim, czytelną i trwałą techniką,
- 1.5. ma obejmować całość zamówienia.

2. Opis przedmiotu zamówienia:

2.1. Zakres:

2.1.1. dokonanie oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji, w tym przetwarzania danych osobowych, z obowiązującymi aktami prawnymi, w szczególności:

a) § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2016 r. poz. 113 i 1744),

b) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) i wydanymi do niej rozporządzeniami wykonawczymi,

c) normami bezpieczeństwa,

d) wymaganiami technologicznymi w systemach informatycznych zapewniającymi bezpieczeństwo zasobów sprzętowych i informacyjnych;

2.1.2. przeprowadzenie audytu bezpieczeństwa informacji we wszystkich obszarach funkcjonowania Urzędu Gminy Piątnica, w szczególności w zakresie:

a) organizacyjnym, obejmującym m.in.

- regulacje w obszarze zarządzania bezpieczeństwem informacji,

- dokumentacje, w tym z zakresu ochrony danych osobowych,

- odpowiedzialność za bezpieczeństwo informacji i koordynację prac związanych

z zarządzaniem bezpieczeństwem informacji,

- przeprowadzenie wywiadów z pracownikami;

b) fizycznym i środowiskowym, w tym:

- weryfikacja granic obszaru bezpiecznego,

- weryfikacja zabezpieczeń wejścia/wyjścia,

- weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń,

- weryfikacja bezpieczeństwa okablowania strukturalnego,

- weryfikacja systemów chłodzenia,

- weryfikacja systemów alarmowych;
- c) teleinformatycznym, z uwzględnieniem:
 - weryfikacji istniejących procedur zarządzania systemami teleinformatycznymi,
 - weryfikacji ochrony przed oprogramowaniem szkodliwym,
 - weryfikacji procedur zarządzania kopiami zapasowymi,
 - weryfikacji procedur związanych z rejestracją błędów,
 - weryfikacji procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania,
 - weryfikacji zabezpieczeń stacji roboczych i nośników danych, w szczególności tych, na których przetwarzane są dane osobowe,
 - weryfikacji haseł (ich stosowanie, przyjęta polityka ich tworzenia oraz zmiany, mechanizmy ich przechowywania),
 - weryfikacji zabezpieczeń urządzeń na styku sieci wewnętrznej z siecią publiczną (testy penetracyjne, testowanie podatności na ataki z zewnątrz, ataki naśladujące działalność hakera próbującego przejąć kontrolę nad systemami, bądź uzyskanie dostępu do zasobów serwerów),
 - analizy i oceny mechanizmów zarządzania aktualizacjami;
- d) socjotechnicznym czynnika ludzkiego, polegającym na:
 - sprawdzeniu sposobu przechowywania haseł przez użytkowników,
 - weryfikacji ochrony powierzonego sprzętu i dokumentacji,
 - weryfikacji wiedzy pracowników nt. zasad ochrony danych osobowych i bezpieczeństwa teleinformatycznego;
- e) analizy szacowania ryzyka w oparciu o normę PN-ISO/IEC 27005, uwzględniającego:
 - inwentaryzację aktywów podlegających szacowaniu ryzyka,
 - określenie zagrożeń dla wyznaczonych aktywów,
 - określenie podatności dla wyznaczonych aktywów,
 - określenie prawdopodobieństw dla wyznaczonych aktywów,
 - oszacowanie ryzyka pod kątem skutków naruszenia bezpieczeństwa informacji;

2.1.3. sporządzenie i dostarczenie raportu z audytu w wersji elektronicznej edytowalnej oraz 3 egzemplarzy w wersji papierowej; opracowany raport audytu, wraz z opisem dowodów, zawierać ma m.in.:

- a) ocenę stopnia spełnienia wymogów wymienionych w § 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2016 r. poz. 113 i 1744);
- b) ocenę stopnia spełnienia wymogów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) i wydanych do niej rozporządzeń wykonawczych;
- c) ocenę spełnienia skuteczności stosowanych zabezpieczeń;
- d) wskazanie obszarów wymagających doskonalenia;
- e) określenie zakresu i priorytetu działań naprawczych.

Raport audytu zostanie omówiony z kadrą kierowniczą Urzędu w dniu podpisania protokołu odbioru zamówienia, lub w innym uzgodnionym terminie poprzedzającym podpisanie protokołu odbioru, nie wcześniej jednak niż przed zakończeniem prac przewidzianych w niniejszym zaproszeniu;

2.1.4. opracowanie dokumentacji wymienionej w § 1 pkt 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), tj.

- a) Polityki Bezpieczeństwa,
 - b) Instrukcji Zarządzania Systemem Informatycznym,
- wraz z wymaganymi procedurami i instrukcjami, takimi jak np. Instrukcja alarmowa, stanowiącymi załączniki do dokumentów wymienionych w lit. a i b, bądź odrębne dokumenty;

2.1.5. opracowanie wskazań dla Gminy Piątnica i Urzędu Gminy Piątnica w związku z wdrożeniem 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, zawierających zwłaszcza:

- a) wskazanie działań niezbędnych do płynnego wdrożenia przepisów rozporządzenia, wraz z ich uzasadnieniem,
- b) wskazanie nowych dokumentów, które muszą zostać opracowane,
- c) wskazanie dokumentów, które należy dostosować i zakresu ich dostosowania,
- d) wskazanie niezbędnych i pożądaných regulacji wewnętrznych, które winny być podjęte,
- d) sporządzenie harmonogramu wdrożenia nowych przepisów obejmującego okres od 1.01.2017 r. do 30.06.2018 r.;

2.1.6. szkolenie pracowników z zakresu bezpieczeństwa informacji i ochrony danych osobowych, obejmujące:

- a) omówienie zasad bezpieczeństwa informacji, wynikających z Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym,
- b) omówienie zagrożeń bezpieczeństwa informacji,
- c) zapoznanie ze skutkami naruszeń zasad bezpieczeństwa informacji,
- d) przedstawienie stosowania środków zapewniających bezpieczeństwo informacji,
- e) przedstawienie zasad zgłaszania i reagowania na incydenty.

2.2. Warunki realizacji zamówienia:

2.2.1. szczegółowe parametry zamówienia:

- 1) ilość pracowników: 32,
- 2) ilość lokalizacji: 1,
- 3) ilość serwerów: 4,
- 4) ilość stacji komputerowych: 34,
- 5) ilość stacji komputerowych bez dostępu do sieci wewnętrznej urzędu: 3;

2.2.2. zadania opisane w pkt 2 i pkt 6 należy przeprowadzić w siedzibie Zamawiającego;

2.2.3. o udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy posiadają niezbędną wiedzę i doświadczenie oraz dysponują odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia, tj.

a) Wykonawca zobowiązany jest wykazać iż, w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy — w tym okresie, należycie zrealizował co najmniej 2 zamówienia polegające na przeprowadzeniu audytu bezpieczeństwa informacji, zgodnie z wymaganiami zawartymi w KRI, o wartości co najmniej 10000,00 zł brutto każde

[UWAGA! przez jedną usługę Zamawiający rozumie jeden/ą kontrakt/umowę],

b) Wykonawca zobowiązany jest wykazać, że dysponuje co najmniej 2 osobami które będą uczestniczyć w wykonywaniu zamówienia, z których każda posiada co najmniej:

- wykształcenie wyższe;
- certyfikat audytora wiodącego ISO/IEC 27001:2013 (kurs akredytowany w IRCA tj. „International Register of Certified Auditors”);
- doświadczenie w przeprowadzaniu co najmniej 2 audytów certyfikujących zgodnych z KRI.

Ocena spełniania wyżej wymienionych warunków udziału w zapytaniu będzie dokonana w oparciu o treść dokumentów, o których mowa w pkt 6 zapytania, na zasadzie „spełnia” lub „nie spełnia” wymaganego warunku.

Oferty Wykonawców, którzy nie spełnią ww. warunków nie będą oceniane

3. Wymagany termin realizacji zamówienia: do 22.12.2016 r.

4. Termin płatności: 14 dni od prawidłowo wystawionej faktury.

5. Przy wyborze propozycji do realizacji zamawiający będzie się kierował kryterium:

Cena brutto – 100 %

6. Propozycja ma zawierać następujące dokumenty:

- 6.1. formularz propozycji cenowej wg. załączonego wzoru,
- 6.2. kserokopię aktualnego wpisu do właściwego rejestru, uprawniającego wykonawcę do występowania w obrocie prawnym, (potwierdzoną za zgodność z oryginałem przez wykonawcę),
- 6.3. wypełniony i zaparafowany wzór umowy,
- 6.4. wykaz osób uczestniczących w wykonaniu zamówienia, zawierający:
 - imię i nazwisko,
 - rolę w realizacji zamówienia (audytor wiodący, informatyk, audytor),
 - kwalifikacje zawodowe (doświadczenie zawodowe w latach, wykaz certyfikatów),
- 6.5. wykaz wykonanych usług, o których mowa w ust. 5 pkt 1 lit. a.

7. Opis sposobu obliczenia ceny w składanej propozycji cenowej:

W cenę propozycji należy wliczyć:

- 1/ wartość usługi/dostawy,
- 2/ obowiązujący podatek od towarów i usług.

Cena podana przez wykonawcę za świadczoną usługę lub dostawę jest obowiązująca przez okres ważności umowy i nie będzie podlegała waloryzacji w okresie jej trwania. Zamawiający wybierze propozycję odpowiadającą wszystkim postawionym przez niego wymogom i o najniższej cenie.

8. Miejsce i termin złożenia propozycji cenowej:

8.1. Propozycję cenową należy złożyć w terminie do dnia: **29 listopada 2016 r. do godziny 12:00.**

8.2. Sposób dostarczenia oferty - można:

1) dostarczyć osobiście pod adres: Urząd Gminy Piątница, ul. Stawiskowska 53, 18-421 Piątница Poduchowna, Kancelaria (parter, pokój nr 8).

Na kopercie należy umieścić nazwę i adres zamawiającego, nazwę i adres wykonawcy oraz napis: „Oferta na wykonanie audytu w zakresie bezpieczeństwa informacji”;

2) przesłać pocztą (lub kurierem) pod adres: Urząd Gminy Piątница, ul. Stawiskowska 53, 18-421 Piątница Poduchowna oznaczoną na kopercie - jak w pkt 1.

8.3. Każdy wykonawca może złożyć tylko jedną ofertę.

8.4. Oferta musi być podpisana przez osoby upoważnione do reprezentowania wykonawcy.

9. Osobą uprawnioną do kontaktów jest starszy informatyk – Konrad Majkowski /tel. 86 2162476 w.11/.

10. Informacje dotyczące zawierania umowy:

10.1. W terminie do 7 dni od daty powiadomienia o wyborze propozycji cenowej wybrany wykonawca ma podpisać umowę w siedzibie Zamawiającego, pokój nr 1.

10.2. Umowa musi zawierać wszystkie uwarunkowania złożonej propozycji cenowej.

10.3. Zamawiający zastrzega sobie prawo odstąpienia bądź unieważnienia zapytania ofertowego bez podania przyczyny;

10.4. Zamawiający zastrzega sobie możliwość przeprowadzenia dodatkowych negocjacji z Wykonawcą, którego oferta zostanie uznana za najkorzystniejszą;

10.5. Zamawiający zastrzega sobie prawo sprawdzania w toku oceny ofert wiarygodności przedstawionych przez wykonawców dokumentów, wykazów, danych i informacji;

10.6. Zamawiający w związku z prowadzoną procedurą nie dopuszcza możliwości składania ofert częściowych, zamówienie należy traktować całościowo.

W załączeniu:

1. wzór Formularza propozycji cenowej,
2. wzór umowy


.....
(podpis i pieczęć kierownika zamawiającego)