ABI.142.1.2016 **Kobyłka, 12 lipca 2016 r.**

REGULAMIN
konkursu ofert
na wykonanie usługi audytu bezpieczeństwa informacji
w Urzędzie Miasta Kobyłka

wartość zamówienia nie przekracza kwoty 30 000 Euro

I. ZAMAWIAJĄCY

Miasto Kobyłka
ul. Wołomińska 1
05-230 Kobyłka
NIP: 125-133-23-90, REGON: 013269663,
tel. 22 760-70-54 Administrator Bezpieczeństwa Informacji Wojciech Reutt
e-mail: urzad@kobylka.pl wojciech.reutt@kobylka.pl
strona: www.kobylka.pl www.bip.kobylka.pl

II. PROCEDURA

Zamawiający prowadzi postępowanie w trybie dwuetapowego konkursu ofert – art. 4 pkt 8 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz.U. z 2015 r. poz. 2164) (wartość zamówienia nie przekracza kwoty 30 000 Euro).

Postępowanie jest dwuetapowe (*podobne jak w przetargu ograniczonym*):

ETAP I składanie wniosków i wybór 7 wykonawców dopuszczonych do składania ofert

ETAP II składanie ofert i wybór wykonawcy realizującego zamówienie

III. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest audyt bezpieczeństwa informacji (zwłaszcza danych osobowych i bezpieczeństwa teleinformatycznego) w Urzędzie Miasta Kobyłka.
Wstępny, szczegółowy, minimalny zakres przedmiotu zamówienia stanowi załącznik nr 1 do niniejszego regulaminu. Wykonawca może zaproponować poszerzenie zakresu zamówienia (kryterium kwalifikacyjne trzecie).

IV. TERMIN WYKONANIA ZAMÓWIENIA

Wykonawca zrealizuje przedmiot zamówienia (w tym ew. oferowane poszerzenia) do 31.05.2017 r. (płatności etapowo; zamawiający zapłaci 40% ceny oferty po zakończeniu realizacji przedmiotu zamówienia) wg harmonogramu rzeczowo-finansowego ustalonego w ofercie a uszczegółowionego w ramach formalności przed podpisaniem umowy.

V. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ OPIS SPOSOBU DOKONYWANIA OCENY SPEŁNIANIA TYCH WARUNKÓW

1. O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy spełniają następujące warunki udziału w postępowaniu:
   1) posiadają uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania;
   2) posiadają wiedzę i doświadczenie w przedmiocie zamówienia;
   3) dysponują odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia;
   4) znajdują się w sytuacji ekonomicznej i finansowej umożliwiającej realizację przedmiotu zamówienia.
2. Sposób dokonywania oceny spełniania warunków udziału w postępowaniu:
   1) w celu spełnienia warunku wymienionego w ust. 1 pkt 2 wykonawca winien wykazać wykonanie w okresie ostatnich trzech lat przed upływem terminu składania wniosków, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, usług w zakresie wykonania audytów, łącznie:
      a) audyty danych osobowych łącznie w:
         — co najmniej 1 urzędzie państwowym centralnym (to jest: ministerstwo, urząd naczelny/centralny podległy ministrowi lub premierowi) lub oddziale wojewódzkim takiego urzędu lub ambasadzie lub centralnym organie państwowym (NIK, KRRiT, RPO, NBP) lub jego oddziale wojewódzkim lub aktualnym urzędzie wojewódzkim lub marszałkowskim lub urzędzie administracji rządowej terenowej na poziomie województwa (administracji zespolonej lub niezespolonej) lub urzędzie miejskim aktualnego miasta wojewódzkiego lub uczelni wyższej (mającej status uczelni akademickiej) lub państwowej jednostce badawczej oraz
         — urzędach gminy/miasta o liczbie mieszkańców min. 20 tys. lub w urzędach powiatowych lub urzędach administracji rządowej terenowej na poziomie powiatu (administracji zespolonej lub niezespolonej) – łącznie co najmniej 4 takie podmioty,
      b) audyty bezpieczeństwa teleinformatycznego łącznie w:
         — co najmniej 1 podmiocie wymienionym w lit. a tir. pierwszy oraz
         — co najmniej 4 podmiotach wymienionych w lit. a tir. drugi

         Może być doświadczenie z lit. a.

      Wykonawca w kryterium kwalifikacyjnym może wykazać usługi wykazane w warunku wiedzy i doświadczenia (jednak musi wyraźnie w ofercie zaznaczyć, które usługi wypełniają warunek).
   2) w celu spełnienia warunku wymienionego w ust. 1 pkt 3 wykonawca winien wykazać dysponowanie osobami zdolnymi do realizacji zamówienia, to jest łącznie co najmniej:
      a) jedną osobą:
         — posiadającą wiedzę (prawną i praktyczną) z zakresu bezpieczeństwa informacji (zwłaszcza ochrony danych osobowych),
         — posiadającą doświadczenie w przeprowadzenia audytu bezpieczeństwa informacji (zwłaszcza audytu ochrony danych osobowych) tzn. wykonała co najmniej 5 ww. audytów,
         — posiadającą doświadczenie we wdrażaniu systemu Zarządzania Bezpieczeństwem Informacji wg standardu ISO/IEC 27001 oraz
      b) jedną osobą:
         — posiadającą wiedzę (prawną i praktyczną) z zakresu informatyki (zwłaszcza ochrony teleinformatycznej i Krajowych Ram Interoperacyjności),
         — posiadającą doświadczenie w przeprowadzania audytu bezpieczeństwa informacji (zwłaszcza audytu ochrony teleinformatycznej) tzn. wykonała co najmniej 5 ww. audytów oraz

c) jedną osobą będącą czynnym radcą prawnym lub adwokatem posiadającą wiedzę z zakresu bezpieczeństwa informacji (zwłaszcza ochrony danych osobowych i ochrony teleinformatycznej) oraz
d) jedną osobą doświadczoną w przeprowadzaniu szkoleń z zakresu bezpieczeństwa informacji (zwłaszcza ochrony danych osobowych i bezpieczeństwa teleinformatycznego), która zrealizowała co najmniej 8 ww. szkleń dla grupy min. 10 osób (nie szkolenie wewnętrzne wykonawcy).

Powyższe warunki może wypełniać jedna, dwie, trzy lub cztery osoby.

Wykonawca w kryterium kwalifikacyjnym może wykazać osoby wykazane w tym warunku (jednak musi wyraźnie w ofercie zaznaczyć, które osoby „wypełniają" ww. warunek).

3. Wykonawcy niespełniający wszystkich warunków zostaną wykluczeni z postępowania.
4. Wykonawca dołączy do wniosku dokumenty poświadczające spełnianie warunków określonych w ust. 2:
   1) Dokumenty poświadczające należyte wykonanie usługi np. listy referencyjne itp. oraz wykaz – ust. 2 lit. 1;
   2) wykaz – ust. 2 lit. 2.
5. Wykonawca dołączy do wniosku szczegółowy opis swojej firmy.

VI. SPOSÓB WYBORU 7 WYKONAWCÓW DO II ETAPU

1. Do drugiego etapu dopuszczeni zostaną wykonawcy wg poniższych kryteriów kwalifikacyjnych:

- doświadczenie - 53%
- proponowane poszerzenie zakresu przedmiotu zamówienia - 18%
- dysponowanie osobami - 18%
- posiadanie certyfikatu Microsoft (certyfikowane uprawnienia wydane przez firmę Microsoft do weryfikowania legalności oprogramowania) - 4%
- posiadanie wdrożonego systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001 - 4%
- posiadana zdolność finansowa - 3%

2. Do drugiego etapu zostanie zakwalifikowanych 5 wykonawców, którzy uzyskają największą łączną liczbę punktów (przyznanych na poniższych zasadach) oraz 2 kolejnych z największą liczbą punktów w kryterium kwalifikacyjnym doświadczanie, którzy mają certyfikat Microsoft (certyfikowane uprawnienia wydane przez firmę Microsoft do weryfikowania legalności oprogramowania).

   Do drugiego etapu nie zostaną dopuszczeni wykonawcy, których działalność będzie budziła uzasadnione wątpliwości zamawiającego.

   http://giodo.gov.pl/560/id_art/9197/j/pl

   Oferty ich zostaną odrzucone.
3. Przed kwalifikacją zamawiający, na podstawie złożonych wniosków, opracuje (uszczegółowi) przedmiot zamówienia i prześle go wybranym wykonawcom. Jeżeli wybrany wykonawca nie akceptuje części lub całości poszerzonego zakresu przedmiotu zamówienia (obowiązującego) może przekazać zamawiającemu swoje uwagi w tym zakresie. Jeżeli zamawiający podtrzyma zakres, dany wykonawca może zrezygnować z uczestnictwa w drugiej turze, zaś na jego miejsce zostanie wybrany kolejny wykonawca na powyższych zasadach.
4. Sposób przyznawania punktów w kryterium kwalifikacyjnym doświadczenie

   Doświadczenie, które wykonawca wykaże w celu kwalifikacji do drugiego etapu musi być doświadczeniem własnym wykonawcy (niepożyczonym). Wykonawca musi dołączyć wykaz tabelaryczny wymienianego doświadczenia wskazując, do jakiej z poniższych kategorii należy dana usługa.

Wykonawca w kryterium kwalifikacyjnym może wykazać usługi wykazane w warunku wiedzy i doświadczenia (jednak musi wyraźnie w ofercie zaznaczyć, które usługi wypełniają warunek).

1) Doświadczenie w zakresie audytu ochrony danych osobowych (mogą być usługi z pkt 2 lub 3)
   a) w urzędzie państwowym centralnym (to jest: ministerstwo, urząd naczelny/centralny podległy ministrowi lub premierowi) lub ich oddziały wojewódzkie lub ambasady lub centralne organy państwowe (NIK, KRRiT, RPO, NBP itp.) lub ich oddziały wojewódzkie lub aktualne urzędy wojewódzkie lub marszałkowskie lub urzędy administracji rządowej terenowej na poziomie województwa (zespolonej lub niezespolonej) lub urzędy miejskie aktualnego miasta wojewódzkiego lub uczelnie wyższe (mającą status uczelni akademickiej) lub państwowe jednostki badawcze
      20 pkt. za każdy audyt,
   b) w urzędzie gminy/miasta o liczbie mieszkańców min. 20 tys. lub urzędzie powiatowym (inne niż w lit. a) lub urzędzie administracji rządowej terenowej na poziomie powiatu (zespolonej lub niezespolonej) lub w podmiocie prywatnym zatrudniającym powyżej 200 osób
      7 pkt. za każdy audyt,
   c) podmioty prywatne o liczbie zatrudnionych pomiędzy 80 a 200 osób lub inne instytucje publiczne
      3 pkt. za każdy audyt,
   d) audyty w podmiotach innych niż ww.
      1 pkt za każdy audyt;

2) Doświadczenie w zakresie audytu bezpieczeństwa teleinformatycznego (mogą być usługi z pkt 1 lub 3)
   a) w urzędzie państwowym centralnym (to jest: ministerstwo, urząd naczelny/centralny podległy ministrowi lub premierowi) lub ich oddziały wojewódzkie lub ambasady lub centralne organy państwowe (NIK, KRRiT, RPO, NBP) lub ich oddziały wojewódzkie lub aktualne urzędy wojewódzkie lub marszałkowskie lub urzędy administracji rządowej terenowej na poziomie województwa (zespolonej lub niezespolonej) lub urzędy aktualnego miasta wojewódzkiego lub uczelnie wyższe (mającą status uczelni akademickiej) lub państwowe jednostki badawcze
      15 pkt. za każdy audyt,
   b) urząd gminy/miasta o liczbie mieszkańców min. 20 tys. lub urząd powiatowy (inne niż w lit. a) lub urzędy administracji rządowej terenowej na poziomie powiatu (zespolonej lub niezespolonej) lub podmioty prywatne zatrudniające powyżej 200 osób
      5 pkt. za każdy audyt,
   c) podmioty prywatne o liczbie zatrudnionych pomiędzy 80 a 200 osób lub inne instytucje publiczne
      2 pkt za każdy audyt,
   d) audyty w podmiotach innych niż ww.
      0,5 pkt za każdy audyt;

3) Doświadczenie w zakresie wdrożenia systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001 – (mogą być usługi z pkt 1 lub 2)
   a) za przeprowadzenie audytu bezpieczeństwa danych osobowych w urzędzie państwowym centralnym (to jest: ministerstwo, urząd naczelny/centralny podległy ministrowi lub premierowi) lub ich oddziały wojewódzkie lub ambasady lub centralne organy państwowe (NIK, KRRiT, RPO, NBP) lub ich oddziały wojewódzkie lub aktualne urzędy wojewódzkie lub marszałkowskie lub urzędy administracji rządowej terenowej na poziomie województwa (zespolonej lub

niezespolonej) lub urzędy aktualnego miasta wojewódzkiego lub uczelnie wyższe (mającą status uczelni akademickiej) lub państwowe jednostki badawcze
5 pkt. za każdy audyt,

b) urząd gminy/miasta o liczbie mieszkańców min. 20 tys. lub urząd powiatowy (inne niż w lit. a) lub urzędy administracji rządowej terenowej na poziomie powiatu (zespolonej lub niezespolonej) lub podmioty prywatne zatrudniające powyżej 200 osób
1,5 pkt. za każdy audyt,

c) podmioty prywatne o liczbie zatrudnionych pomiędzy 80 a 200 osób lub inne instytucje publiczne
0,5 pkt. za każdy audyt,

d) audyty w podmiotach innych niż ww.
0,25 pkt. za każdy audyt.

A następnie punkty zostaną przeliczone na podstawie wzoru:

D = db / dn * 100 * 53%
D - liczba punktów przyznanych w kryterium kwalifikacyjnym doświadczenie
db - liczba punktów przyznanych na podstawie pkt 1-3 ofercie badanej
dn - największa liczba punktów przyznanych na podstawie pkt 1-3

5. Proponowane poszerzenie zakresu przedmiotu zamówienia
Wykonawca może dołączyć do wniosku opis (maksymalnie 5 stron formatu A4 zapisanych czcionką Times New Roman, rozmiar 12, odstęp 1,5), na których wykonawca zaproponuje poszerzenie zakresu przedmiotu zamówienia ponad minimalny.
Każdy z członków komisji oceniającej wnioski przyzna od 0 do 18 punktów. Liczba przyznanych punktów wnioskowi będzie średnią arytmetyczną punktów przyznanych przez członków komisji.

6. Dysponowanie osobami
Wykonawcy zostaną przyznane punkty za:
1) Dysponowanie (umowa o pracę, właściciel, członek zarządu) osobami, które pełnią (na dzień składania wniosku) funkcję Administratora Bezpieczeństwa Informacji w innych podmiotach niż wykonawca
9 pkt za każdą ww. osobę
2) Dysponowanie (umowa o pracę, właściciel, członek zarządu) osobami mającymi uprawnienia do wdrażania systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001 (audytor wiodący)
3 pkt za każdą ww. osobę
3) Dysponowanie (umowa o pracę, właściciel, członek zarządu) osobami posiadającymi poświadczenie bezpieczeństwa dostęp do informacji niejawnych o klauzuli tajności „poufne", „tajne" lub „ściśle tajne"
1 pkt za każdą ww. osobę

A następnie punkty zostaną przeliczone na podstawie wzoru:

O = ob / on * 100 * 18%
O - liczba punktów przyznanych w kryterium kwalifikacyjnym dysponowanie osobami
ob - liczba punktów przyznanych na podstawie pkt 1-3 ofercie badanej
on - największa liczba punktów przyznanych na podstawie pkt 1-3

Wykazane osoby nie mogą być użyczone od podmiotu trzeciego. Muszą stanowić zasób osobowy wykonawcy.

7. Posiadany certyfikat Microsoft (certyfikowane uprawnienia wydane przez firmę Microsoft do weryfikowania legalności oprogramowania)

Za posiadanie przez wykonawcę certyfikowanych uprawnień wydanych przez firmę Microsoft do weryfikowania legalności oprogramowania przyznanych zostanie 5 punktów.
Należy złożyć stosowne oświadczenie.
Ww. certyfikat musi dotyczyć wykonawcy składającego wniosek. Nie może być udostępniony („pożyczony") od podmiotu trzeciego.

8. Wdrożony system Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001
   Za wdrożony u wykonawcy system Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001przyznane zostaną 4 pkt. Uniemożliwia się jakiekolwiek „pożyczanie" od podmiotu trzeciego.
   Należy złożyć stosowne oświadczenie.

9. Zdolność kredytowa, lub posiadane środki
   Wykonawca musi dołączyć do wniosku stosowny dokument – informację banku lub spółdzielczej kasy oszczędnościowo-kredytowej potwierdzającej wysokość posiadanych środków finansowych lub zdolność kredytową wykonawcy, wystawionej nie wcześniej niż 3 miesiące przed upływem terminu składania wniosków (oryginał lub kopia poświadczona przez wykonawcę za zgodność z oryginałem).

   A następnie przyzna punkty wg wzoru

   Zk = zko / zkn * 100 * 9%
   Zk - liczba punktów przyznanych w kryterium zdolność kredytowa lub posiadane środki
   zkb- zdolność kredytowa lub posiadane środki w ofercie badanej
   zkn- największa zdolność kredytowa lub posiadane środki

   Zamawiający uniemożliwia oparcie się na zdolności finansowej podmiotu trzeciego. Wykazana zdolność kredytowa lub posiadane środki muszą być zdolnością lub środkami własnymi wykonawcy (ew. konsorcjum).

10. Wykonawca chcąc otrzymać punkty kwalifikujące do drugiego etapu dołącza do wniosku wyłącznie stosowne oświadczenia i wykazy (poza opisem w kryterium kwalifikacyjnym Proponowane poszerzenie zakresu przedmiotu zamówienia i zdolnością kredytową). Szczegółowa weryfikacja doświadczenia i uprawnień/certyfikatów wykonawcy i wykazanych osób będzie przeprowadzona w stosunku do wykonawców, którzy zakwalifikują się do drugiego etapu. Po ustaleniu opisu przedmiotu zamówienia i ostatecznej kwalifikacji zamawiający wskaże termin 7 dni na przedłożenie stosownych dokumentów (w wyjątkowych sytuacjach, zwłaszcza w doświadczeniu, możliwa jest weryfikacja telefoniczna).

VII. SPOSÓB WYBORU WYKONAWCY W II ETAPIE

1. Zamawiający po opublikowaniu 7 wykonawców wybranych do drugiego etapu, zażąda od nich dokumentów poświadczających otrzymane punkty w kryteriach kwalifikacyjnych (rodz. VI ust. 10).
2. Zamawiający przekaże wybranym w I etapie wykonawcom:
   1) po otrzymaniu od nich oświadczenia o zachowaniu poufności
      a) Politykę bezpieczeństwa,
      b) Instrukcje zarządzania systemem informatycznym,
      c) *do wglądu (**wymagana** wizyta osobista przedstawiciela wykonawcy)* dokumentacja Administratora Bezpieczeństwa Informacji;
   2) uszczegółowiony opis przedmiotu zamówienia (opracowany na podstawie dołączonych do wniosków proponowanych poszerzeń zakresu przedmiotu zamówienia);
   3) uszczegółowione kryteria oceny ofert;

4) pytania/kazusy do opracowania w ramach kryterium opracowanie wskazanych problemów

- oraz określi termin składania ofert (14-30 dni).

3. Wykonawca będzie mógł zadać pytania do uszczegółowionych opisu przedmiotu zamówienia i kryteriach oceny ofert.

VIII. OPIS SPOSOBU PRZYGOTOWANIA WNIOSKU I OFERTY

1. Wykonawca sam opracowuje wniosek i ofertę. Wykonawca obowiązkowo musi dołączyć do wniosku wykazy w formie tabelarycznej, w których wyraźnie uwidoczni (opisze) cechy wykazanych usług i osób oraz załączy odpowiednie certyfikaty, które umożliwią przypisanie odpowiedniej liczby punktów w kryteriach kwalifikacyjnych.
2. Wniosek powinien być:
   - opatrzony pieczątką firmową,
   - posiadać datę sporządzenia,
   - zawierać adres lub siedzibę wykonawcy, numer telefonu, numer NIP, e-maila,
   - potwierdzać warunki uczestnictwa w postępowaniu (**niezbędne dokumenty**),
   - podpisany przez wykonawcę (osobę umocowaną),
   - zawierać dokument potwierdzający umocowanie osoby podpisującej wniosek,
   - kryteria kwalifikacyjne – tabelaryczne zestawienie doświadczenia i osób (koniecznie z opisem umożliwiającym przyporządkowanie) oraz oświadczenia,
   - informację banku lub spółdzielczej kasy oszczędnościowo-kredytowej potwierdzającej wysokość posiadanych środków finansowych lub zdolność kredytową wykonawcy, wystawionej nie wcześniej niż 3 miesiące przed upływem terminu składania wniosków, jeżeli wykonawca chce otrzymać punkty w kryterium kwalifikacyjnym zdolność kredytowa lub posiadane środki,
   - jeżeli wykonawca chciałby zaproponować zmianę w kryteriach oceny ofert (rodz. X) może dołączyć do wniosku propozycje zmiany.
3. Oferty powinny być:
   - opatrzone pieczątką firmową,
   - posiadać datę sporządzenia,
   - zawierać adres lub siedzibę wykonawcy, numer telefonu, numer NIP, e-maila,
   - podpisany przez wykonawcę (osobę umocowaną),
   - zawierać dokument potwierdzający umocowanie osoby podpisującej ofertę,
   - zawierać szczegółowy plan rzeczowo-finansowy audytu bezpieczeństw informacji oraz opracowanie problemów/kazusów.
4. Wykonawca wskaże w ofercie numer telefonu, pod którym będzie dostępny w godzinach pracy zamawiającego, przez cały okres trwania umowy.
5. Wniosek i oferta powinny być napisane czytelnie, w języku polskim (wskazany jest maszynopis lub wydruk komputerowy).
6. Wszelkie poprawki lub zmiany w tekście wniosku i oferty muszą być parafowane własnoręcznie przez osobę podpisującą.

IX. MIEJSCE ORAZ TERMIN SKŁADANIA WNIOSKÓW UCZESTNICTWA.

1. Wniosek powinien być przesłany za pośrednictwem: poczty lub kuriera na adres: Urząd Miasta Kobyłka, 05-230 Kobyłka ul. Wołomińska 1 lub też dostarczona osobiście do kancelarii Urzędu Miasta Kobyłka, do dnia **26.07.2016r. do godz. 13^{00}, otwarcie wniosków 13^{15}**

   W przypadku przesłania wniosku lub oferty pocztą lub przesyłką kurierską do zamawiającego, należy wziąć pod uwagę, że terminem jej dostarczenia (złożenia) zamawiającemu jest jej wpływ do miejsca oznaczonego przez zamawiającego, jako miejsce składania wniosków lub ofert (nie termin nadania). Zamawiający nie bierze odpowiedzialności za nieterminowe doręczanie korespondencji.

2. Wniosek wraz z załącznikami należy złożyć w zapakowanej kopercie oznaczonej:

WNIOSEK
wykonanie usługi audytu bezpieczeństwa informacji
w Urzędzie Miasta Kobyłka
nie otwierać przed 26.07.2016 r. godz. 13:15.

3. Wnioski i oferty złożone po terminie nie będą rozpatrywane.
4. Wykonawca może przed upływem terminu składania ofert zmienić lub wycofać swoją ofertę lub wniosek.
5. W toku badania i oceny wniosków lub ofert Zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych wniosków lub ofert.
6. Zamawiający zastrzega sobie unieważnienie postępowania na każdym etapie bez podania przyczyny.

X. SPOSÓB OCENY OFERT

1. Planowane kryteria oceny ofert:

cena ofertowa	–	ok. 40%,
ocena planu audytu	–	ok. 25%
podwyższenie bezpieczeństwa	–	ok. 20%
opracowanie wskazanych problemów	–	ok. 15%

Zamawiający uszczegółowi kryteria oceny ofert po zamknięciu 1 etapu postępowania i przekaże je wybranym wykonawcom wraz z uszczegółowionym opisem przedmiotu zamówienia.

2. Za najkorzystniejszą ofertę zostanie wybrana oferta z największą łączną liczbą punktów.
3. Sposób obliczania punktacji:

Po = Co + Pa + Pb + Wp

Po – punktacja oferty

Co – liczba punktów w kryterium cena oferty

Pa – liczba punktów w kryterium ocena planu audytu

Pb – liczba punktów w kryterium podwyższenie bezpieczeństwa

Wp – liczba punktów w kryterium opracowanie wskazanych problemów

Kryterium – cena ofertowa

Wykonawca poda cenę oferty (z właściwym podatkiem od towarów i usług) za realizację przedmiotu zamówienia wyrażoną w polskiej walucie.

Punkty zostaną przyznane wykonawcy wg wzoru:

$$Co = C_n / C_b * 100 * 40\%$$

gdzie:	Co	–	ilość przyznanych punktów w kryterium cena
	C_n	–	cena brutto najniższej oferty
	C_b	–	cena brutto badanej oferty

Kryterium – ocena planu audytu

Wykonawca do oferty musi dołączyć szczegółowy plan rzeczowo-finansowy. Wykonawca będzie nim związany w cenie ofertowej. Zamawiający dopuszcza zmiany w ww. planie do 30%, wówczas strony ustalą wysokość wynagrodzenia.
Plan rzeczowo-finansowy musi być spójny z ostatecznym opisem przedmiotu zamówienia, jednak wykonawca może zaoferować zakres szerszy.
Oceniane będą (kolejność wg wagi):
- szczegółowość planu (doszczegółowienie opisu przedmiotu zamówienia np. sposób realizacji analiz teleinformatycznych),
- podział na etapy (przejrzyste podzielenie przedmiotu zamówienia na etapy i określenie jasnych mierników zrealizowania danego etapu),
- rozłożenie realizacji w czasie – wykonawca może skrócić czas realizacji przedmiotu zamówienia, jednak zamawiający oczekuje stopniowego równomiernego rozłożenia płatności 60% ceny oferty, zaś faktura za pozostałe 40% musi być wystawiona nie wcześniej niż w styczniu 2017 roku (realizacja szkolenia końcowego nie wcześniej niż w grudniu 2016 r.)
- poszerzenie przedmiotu zamówienia.

Każdy z członków komisji oceniającej oferty przyzna od 0 do 25 punktów. Liczba przyznanych punktów ofercie będzie średnią arytmetyczną punktów przyznanych przez członków komisji.

Kryterium – podwyższenie bezpieczeństwa

W związku z faktem, że wybrany wykonawca będzie miał dostęp do teleinformatycznych zabezpieczeń zamawiającego oraz do sposobu ochrony danych osobowych wykonawcy, którzy zaoferują wykonanie przedmiotu zamówienia przez osoby mające aktualne poświadczenie bezpieczeństwa o klauzuli minimum „poufne" otrzymają puenty w tym kryterium na poniższych zasadach:

1. Za oferowanie wykonania całości przedmiotu zamówienia wyłącznie przez ww. osoby wykonawca otrzyma 20 pkt.
2. Za oferowanie wykonania całości audytu teleinformatycznego oraz ocenę i opracowanie nowych dokumentów związanych z ochroną danych osobowych wyłącznie przez ww. osoby wykonawca otrzyma 17 pkt.
3. Za oferowanie wykonania całości audytu teleinformatycznego wyłącznie przez ww. osoby wykonawca otrzyma 15 pkt.
4. Za oferowanie nadzorowania wykonania całości przedmiotu zamówienia (min. pozytywna opinia o osobach wykonujących przedmiot zamówienia, opracowanie planu działań spójnego ze złożonym do oferty, pisemna ocena wyników audytu z propozycjami działań) wyłącznie przez ww. osoby wykonawca otrzyma 10 pkt.
5. Za oferowanie wykonania oceny i opracowania nowych dokumentów związanych z ochroną danych osobowych wyłącznie przez ww. osoby wykonawca otrzyma 5 pkt.

Wykazane osoby nie mogą być użyczone od podmiotu trzeciego. Muszą stanowić zasób osobowy wykonawcy.

Kryterium – opracowanie wskazanych problemów:

Wybranym do drugiego etapu wykonawcom zamawiający przekaże problemy (kazusy) związane z przedmiotem zamówienia (maksymalnie 3). Wykonawca dołączy do oferty ich opracowanie.
Oceniane będą (kolejność wg wagi):
- szczegółowość odpowiedzi i wyczerpanie tematu,
- uzasadnienie proponowanego rozwiązania,
- spojrzenie na problem „wielopłaszczyznowo" (z „punktu widzenia" kilku ustaw),

- powołanie się na orzecznictwa sądów i administracji oraz opinie urzędów centralnych, w tym wskazanie linii orzeczniczej oraz podanie wyjątków od tej linii.
Każdy z członków komisji oceniającej oferty przyzna od 0 do 15 punktów. Liczba przyznanych punktów ofercie będzie średnią arytmetyczną punktów przyznanych przez członków komisji.

MINIMALNY OPIS PRZEDMIOTU ZAMÓWIENIA
wraz z <u>proponowanymi</u> poszerzeniami (opcjonalnie)

1. Przedmiotem zamówienie jest usługa polegająca na przeprowadzeniu audytu bezpieczeństwa informacji zgodnie z rozporządzeniem 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 (Dz. U. z 2016, poz. 113). Po przeprowadzeniu audytu wykonawca musi sporządzić dokument podsumowujący, zawierający propozycje działań dla zamawiającego z podziałem na działania niezbędne, wskazane i opcjonalne (podając uzasadnienie merytoryczne i prawne oraz szacunkowe koszty). Audyt musi obejmować dwie płaszczyzny: bezpieczeństwo teleinformatyczne i ochronę danych osobowych (w tym ochronę wizerunku). Audyt musi obejmować:
   1) audyt zabezpieczeń styku sieci lokalnej i Internet w zakresie wszystkich warstw modelu ISO OSI:
      a) analiza urządzeń zapewniających Zamawiającemu dostęp do sieci Internet w tym urządzenia aktywne oraz urządzenia pasywne,
      b) analiza istniejącej na dzień przeprowadzenia audytu konfiguracji sieci lokalnej,
      c) analiza parametrów technicznych urządzeń, o których mowa w pkt 1lit. a,
      d) analiza oprogramowania wykorzystywanego przez Zamawiającego w zakresie zabezpieczenia teleinformatycznego.
   2) audyt bezpieczeństwa infrastruktury oraz serwerów:
      a) analiza budowy logicznej sieci Zamawiającego – podział na segmenty (fizyczne lub logiczne, o ile istnieją u Zamawiającego),
      b) analiza sposobu połączenia segmentów pomiędzy sobą,
      c) analiza metody komunikacji pomiędzy segmentami sieci,
      d) analiza bezpieczeństwa serwerów;
   3) audyt kopii zapasowych:
      a) analiza poprawności wykonywanych kopii zapasowych,
      b) analiza częstotliwości wykonywania kopii zapasowych,
      c) analiza bezpieczeństwa wykonywanych kopii zapasowych;
   4) audyt zabezpieczeń oraz zainstalowanego oprogramowania:
      a) analiza zainstalowanego oprogramowania znajdującego się na urządzeniach (w tym urządzeniach mobilnych np. laptopy, tablety, *smartfony – możliwe poszerzenie*) Zamawiającego,
      b) analiza bezpieczeństwa stacji roboczych Zamawiającego;
   5) audyt podatności systemów informatycznych Zamawiającego;
   6) inwentaryzacja sprzętu komputerowego;
   7) inwentaryzacja zbiorcza zainstalowanego oprogramowania;
   8) inwentaryzacja zainstalowanego oprogramowania per komputer;
   9) analiza poziomu wdrożenia dokumentacji związanej z ochroną danych osobowych w odniesieniu do stanu faktycznego systemu informatycznego Urzędu oraz ustawy o ochronie danych osobowych:
      a) analiza zgodności przetwarzania danych osobowych z wymogami ustawy o ochronie danych osobowych oraz wewnętrznymi regulacjami,
      b) badanie poziomu wdrożenia polityki bezpieczeństwa informacji Zamawiającego oraz jej zgodności z obowiązującymi przepisami prawa;
      c) czynności powyższe wykonane zostaną po przedstawieniu przez Zamawiającego dokumentów opracowanych przez Zamawiającego dotyczących ochrony danych osobowych – tj. Polityki bezpieczeństwa informacji, Instrukcji zarządzania systemem informatycznym oraz załączników do wymienionej dokumentacji.
   10) analiza poziomu wdrożenia dokumentacji z zgodnie z rozporządzeniem 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;

11) *Badanie - ankieta z użytkownikami mającej na celu weryfikację wiedzy oraz świadomości w zakresie bezpieczeństwa informatycznego oraz ochrony danych osobowych – opcjonalnie*;
12) *audyt wykorzystywania sprzętu komputerowego.*
Analiza wykorzystania sprzętu komputerowego Zamawiającego przez użytkowników w okresie minimum 14 dni roboczych w zakresie przeglądanych stron www, czasu korzystania przez z poszczególnych aplikacji bądź pakietów aplikacji.
opcjonalnie

2. Audyt bezpieczeństwa informacji we wszystkich obszarach funkcjonowania organizacji.
   1) audyt organizacyjny
      a) regulacje w obszarze zarządzania bezpieczeństwem informacji,
      b) odpowiedzialność za bezpieczeństwo informacji i koordynacja prac związanych z zarządzaniem bezpieczeństwem informacji,
      c) dokumentacja w tym z zakresu ochrony danych osobowych,
      d) Przeprowadzenie wywiadów z wybranymi pracownikami;
   2) audyt fizyczny i środowiskowy:
      a) weryfikacja granic obszaru bezpiecznego,
      b) weryfikacja zabezpieczeń wejścia/wyjścia,
      c) weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń,
      d) weryfikacja bezpieczeństwa okablowania strukturalnego;
      e) weryfikacja systemów chłodzenia,
      f) weryfikacja systemów alarmowych;
   3) audyt teleinformatyczny
      a) weryfikacja istniejących procedur zarządzania systemami teleinformatycznymi,
      b) weryfikacja ochrony przed oprogramowaniem szkodliwym,
      c) weryfikacja procedur zarządzania kopiami zapasowymi,
      d) weryfikacja procedur związanych z rejestracją błędów,
      e) weryfikacja procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania,
      f) weryfikacja zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe,
      g) weryfikacja haseł (ich stosowanie, przyjęta polityka ich tworzenia oraz zmiany, mechanizmy ich przechowywania),
      h) analiza i ocena mechanizmów zarządzania aktualizacjami;
3. Zewnętrzne i wewnętrzne testy penetracyjne infrastruktury informatycznej
   1) testy styku sieci lokalnej z Internetem przeprowadzane ze stacji roboczej podłączonej do sieci Internet
      a) analiza topologii brzegu sieci,
      b) weryfikacja mechanizmów ochronnych,
      c) próba wykrycia usług sieciowych udostępnianych do Internetu,
      d) detekcja wersji oraz typu oprogramowania dostępnego z sieci Internet,
      e) eksploitacja dostępnych urządzeń oraz usług wystawionych do sieci Internet,
      f) przedstawienie rozwiązań zwiększających bezpieczeństw styku sieci lokalnej z siecią Internet;
   2) testy penetracyjne przeprowadzone ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego w celu zidentyfikowania możliwości przeprowadzenia włamania z wewnątrz organizacji
      a) analiza topologii sieci LAN,
      b) weryfikacja mechanizmów ochronnych w sieci;
      c) analiza komunikacji sieciowej,
      d) skanowanie portów TCP/UDP próba wykrycia usług sieciowych,
      e) skanowanie hostów aktywnych w sieci,
      f) eksploitacja dostępnych urządzeń oraz usług w sieci LAN,

g) przedstawienie rozwiązań zwiększających bezpieczeństw sieci LAN;

3) audyt socjotechniczny czynnika ludzkiego
   a) próby uzyskania poufnych informacji od użytkowników – *opcjonalnie*,
   b) próby umieszczenia szkodliwego oprogramowania na stacjach roboczych,
   c) próby uzyskania dostępu do danych poufnych u użytkowników– *opcjonalnie*,
   d) sprawdzenie sposobu przechowywania haseł przez użytkowników.
   e) weryfikacja ochrony powierzonego sprzętu i dokumentacji;
4) inwentaryzacja sprzętu i oprogramowania służącego do przetwarzania informacji, *połączona z weryfikacją legalnością użytkowanego oprogramowania – opcjonalnie*.

4. Audyt bezpieczeństwa informacji obejmujący:
   1) Dokumenty do analizy:
      a) Politykę Bezpieczeństwa, Instrukcję Zarządzania Systemem Informatycznym oraz wymagane procedury i instrukcje,
      b) dokumenty ABI'ego,
      c) dokumenty kontroli zarządczej – opcjonalnie,
      d) zakres ubezpieczenia – opcjonalnie,
      e) dokumenty systemu zarządzania jakością zgodnego z normą PN-EN ISO 9001:2009 - opcjonalnie,
      f) Regulamin Organizacyjny UMK + *opcjonalnie inne niezbędne dokumenty*,
      g) zakresy obowiązków osobowych i wydziałów – opcjonalnie,
      h) sposób nadzorowania jednostek w zakresie ochrony danych osobowych i bezpieczeństwa teleinformatycznego pod kątem wypełniania wymogów prawa przez Urząd – zakres opcjonalny, jednak pożądany przez zamawiającego,
      i) informacja niejawna u zamawiającego – zakres opcjonalny,
      j) obieg dokumentów – zakres opcjonalny, jednak pożądany przez zamawiającego,
      k) ochrona tajemnicy przedsiębiorstwa – zakres opcjonalny,
      l) umowy powierzenia danych osobowych,
      m) ochrona fizyczna i techniczna:
         – *umowy z firmą "ochroniarską" – zakres opcjonalny, jednak pożądany przez zamawiającego,*
         – *ocena instalacji alarmowych – zakres opcjonalny,*
      n) ochrona wizerunku w urzędzie (posiadanie wymaganych oświadczeń) – zakres opcjonalny,
      o) ochrona danych osobowych w dokumentacji osobowej (HR) pracowników (w tym Międzyzakładowy Fundusz Świadczeń Socjalnych, kasa zapomogowopożyczkowa, ubezpieczenia grupowe na życie pracowników) – zakres opcjonalny;
   2) Stan faktyczny
      a) sprzęt IT i oprogramowanie (w tym zwłaszcza: Komputery, serwery, telefony komórkowe)
      b) łącza internetowe (w tym bezpieczeństwo fizyczne okablowania),
      c) praktyka pracowników
         – ochrona danych osobowych (wykonawca dokona czynności tak jak w sprawdzeniu z ustawy o ochronie danych osobowych),
         – bezpieczeństwo teleinformatyczne,
      d) sposób ochrony przez firmę zewn.
      e) sposób udostępniania informacji (np. w trybie dostępu do informacji publicznej) – zakres opcjonalny;
   3) Opracowanie zbiorów danych – zakres opcjonalny
      a) ocena kompletności aktualnych zbiorów danych,
      b) wskazanie ew. niezgłoszonych zbiorów – zakres opcjonalny, jednak pożądany przez zamawiającego,
      c) przeprowadzenie sprawdzeń (o których mowa w ustawie o ochronie danych osobowych) wszystkich zbiorów danych.

5. Przygotowanie/opracowanie dokumentów:
   1) Polityka bezpieczeństwa;
   2) Instrukcja ZSI;
   3) nowe dokumenty ABI'ego (formularze) i kontroli zarządczej – zakres opcjonalny;
   4) Polityka zakupowa (w oparciu o PZP, jeżeli zachodzi konieczność stosowania) uwzględniająca szacowane koszty – zakres opcjonalny, jednak pożądany przez zamawiającego:
      a) sprzętu IT
      b) oprogramowania,
      c) *innego wyposażenia urzędu – w tym pomoc w opisie przedmiotu zamówienia (ocena przygotowanych opisów).*
   5) Propozycje zmiany zakresu ubezpieczenia – zakres opcjonalny,
   6) Jeżeli zajdzie taka potrzeba uzupełnienie informacji i wdrożenie zmian odnośnie
      a) kontroli zarządczej – zakres opcjonalny,
      b) systemu zarządzenia jakością zgodnego z normą PN-EN ISO 9001:2009 – zakres opcjonalny,
      c) zakresu obowiązków i Regulaminu Org. UMK,
      d) w innych dokumentach – zakres opcjonalny;
   7) Propozycja zmian, jakie należałoby wykonać:
      a) wdrażając standardy normy ISO/IEC 27001,
      b) wdrażając normę ISO/IEC 27001,
      - wraz z ich wyceną – zakres opcjonalny.
   8) propozycje zmian w nadzorowaniu jednostek w zakresie ochrony danych osobowych i bezpieczeństwa teleinformatycznego (wypełnienie wymogów prawa przez Urząd) – zakres opcjonalny, jednak pożądany przez zamawiającego
   5) opracowanie szczegółowej analizy ryzyka i oszacowanie ryzyk w obrębie badanych zagadnień (*w oparciu o normę PN-ISO/IEC 27005:2014– zakres opcjonalny*):
      a) inwentaryzacja aktywów podlegających szacowaniu ryzyka,
      b) określenie zagrożeń dla wyznaczonych aktywów,
      c) określenie podatności dla wyznaczonych aktywów,
      d) określenie prawdopodobieństw dla wyznaczonych aktywów,
      e) oszacowanie ryzyka pod kątem skutków naruszenia bezpieczeństwa informacji;
   9) wykonanie i przekazanie Raportów z Audytu z omówieniem;
   10) jeżeli zajdzie taka potrzeba odniesienie się we wszystkich ocenach do Krajowych Ram Interoperacyjności;
6. Szkolenie dla pracowników (i ew. osób z jednostek organizacyjnych Miasta Kobyłka – maks. 20 osób z jednostek) obejmujące problematykę:
   1) ochronę danych osobowych i ochronę wizerunku oraz bezpieczeństwa teleinformatycznego w tym:
      a) omówienie zasad bezpieczeństwa informacji,
      b) zagrożenia bezpieczeństwa informacji,
      c) skutki naruszenia zasad bezpieczeństwa informacji,
      d) stosowanie środków zapewniających bezpieczeństwo informacji,
      e) zasady zgłaszania i reagowania na incydenty;
   2) nowe rozwiązania (min. omówienie nowej Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym).

   Osoba szkoląca musi podczas szkolenia przewidywać możliwość zadawania pytań przez uczestników z zakresu przedmiotu zamówienia, a zakres wiedzy osoby szkolącej musi umożliwić jej odpowiedzenie.

   Szkolenie realizowane przez osobę doświadczoną w szkoleniach z zakresu bezpieczeństwa informacji (min. 5 szkoleń w ciągu 12 następujących po sobie miesięcy). W szkoleniu nie może brać udział więcej niż ok. 20-25 osób (uwzględniając liczbę pracowników potrzeba ok. 7 szkoleń).

   Oczekiwany podział grup pracowników:

   - Zarząd Miasta Kobyłka (Burmistrz Miasta, zastępcy burmistrza, Skarbnik Miasta, Sekretarz Miasta),

- dyrektorzy i pracownicy jednostek,
- *radni Miasta Kobyłka – zakres opcjonalny (ocena prawna np. sposobu publikacji i treści uchwał zawierających dane osobowe, transmisji z obrad Rady Miasta),*
- kierownicy wydziałów i stanowiska samodzielne,
- pracownicy tura 1,
- pracownicy tura 2,
- pracownicy tura 3.

7. Zapewnienie opieki doradczej po zakończeniu audytu – zakres opcjonalny.

Wykonawca wskaże jedną osobę odpowiedzialną za koordynację i postęp prac.