ZAPYTANIE OFERTOWE
NA WYKONANIE AUDYTU BEZPIECZEŃSTWA INFORMACJI
W URZĘDZIE MIEJSKIM W GIŻYCKU

Giżycko, 08.07.2016 r.

Zapytanie ofertowe na wykonanie Audytu Bezpieczeństwa Informacji w Urzędzie Miejskim w Giżycku

I. Postanowienia ogólne

W związku z faktem, że Zamawiający planuje przeznaczyć na jego realizację kwotę poniżej wyrażonej w złotych równowartości kwoty 30 000 euro, niniejsze postępowanie – w związku z art. 4 pkt. 8 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity Dz. U. z 2015 r. poz.2164) będzie procedowane na podstawie przepisów Kodeksu cywilnego (art. 70^1 i kolejne).

II. Zamawiający : Gmina Miejska w Giżycku, al. 1 Maja 14, 11-500 Giżycko

III. Opis przedmiotu zamówienia

Wykonanie audytu bezpieczeństwa informacji w Urzędzie Miejskim w Giżycku – opis zadania

I. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest wykonanie audytu bezpieczeństwa informacji w jednostce - Urząd Miejski w Giżycku, al. 1 Maja 14, a w szczególności:

- audyt bezpieczeństwa informacji, systemu zarządzania informacjami,
  -przegląd systemu ochrony technicznej i fizycznej,
  - ocena systemu zabezpieczeń;
- audyt systemów informatycznych, w tym audyt legalności oprogramowania, audyt bezpieczeństwa aplikacji, ochrony i zabezpieczenia danych osobowych (ochrona na poziomie sprzętu i oprogramowania komputerowego oraz infrastruktury,
  - przegląd stacji roboczych, serwerów, urządzeń sieciowych (procesy, autoryzacja, zabezpieczenia, analiza systemu zarządzania kopiami zapasowymi, konfiguracja systemu),
  -przegląd konfiguracji oprogramowania, sieci LAN,
  -inwentaryzacja oprogramowania, dokumentacji licencyjnej,
  - skanowanie,
  -weryfikacja zgodności z KRI;

- audyt zgodności z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (weryfikacja spełnienia przez jednostkę wymagań prawnych i organizacyjnych, związanych z przetwarzaniem danych osobowych),
  - weryfikacja dokumentacji wewnętrznej (kompletność, aktualność).

  Wykonawca przy realizacji przedmiotu zamówienia zobowiązany jest w szczególności do uwzględnienia przepisów oraz wytycznych określonych w:
  - ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
  - ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne,
  -rozporządzeniu 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.

  Audyt winien być zakończony opracowaniem i przekazaniem raportu o stosownym poziomie poufności wraz z projektami niezbędnej zaktualizowanej dokumentacji w formie pisemnej.

  Informacje uzupełniające:

- liczba stacji roboczych (komputerów) w Urzędzie: 110 szt.,
- liczba urządzeń mobilnych (laptopy/tablety): laptopy- 10 szt., tablety 22 szt.,
- liczba serwerów fizycznych 6,
- liczba serwerów wirtualnych 2,
- liczba usług teleinformatycznych ok. 39,
- liczba użytkowanych systemów IT 80,
- liczba pracowników – 83 osoby.

W ramach usługi mają zostać przeprowadzone następujące działania:

I. **Weryfikacja spójności, kompletności i zgodności z przepisami prawa oraz Krajowymi Ramami Interoperacyjności dokumentacji odnoszącej się do:**

- organizacji bezpieczeństwa informacji;
- zarządzania aktywami;
- bezpieczeństwa zasobów ludzkich;
- bezpieczeństwa fizycznego i środowiskowego;
- zarządzania systemami i sieciami;
- kontroli dostępu;
- pozyskiwania, rozwoju i utrzymania systemów informatycznych;

- zarządzania incydentami bezpieczeństwa;
- zarządzania ciągłością działania;
- zgodności z regulacjami.

II. Ocena podatności systemów informatycznych za pomocą profesjonalnego skanera:

1. Przegląd konfiguracji stacji roboczych obejmuje:
   - badanie procesów i metod autoryzacji;
   - weryfikację zarządzanie uprawnieniami i logowaniem zdarzeń;
   - weryfikację zarządzanie zmianami konfiguracyjnymi i aktualizacjami;
   - weryfikację metod autoryzacji na stacjach roboczych;
   - ocenę konfiguracji systemu operacyjnego;
   - weryfikację dostępności i ciągłość działania;
   - analizę systemu zarządzania kopiami zapasowymi;
   - badanie luk komputerów i notebooków;
   - weryfikację zabezpieczeń komputerów przenośnych;
   - weryfikację zasad i procedur użytkowania internetu.

2. Przegląd konfiguracji serwerów obejmuje:
   - proces i metody autoryzacji;
   - weryfikację zarządzanie uprawnieniami i logowaniem zdarzeń;
   - zarządzanie zmianami konfiguracyjnymi i aktualizacjami;
   - ocena konfiguracji systemu operacyjnego serwera;
   - weryfikację dostępności i ciągłości działania;
   - analiza systemu zarządzania kopiami zapasowymi;
   - badanie luk serwerów;
   - analiza bezpieczeństwa funkcji i protokołów specyficznych dla serwera.

3. Przegląd konfiguracji urządzeń sieciowych obejmuje:
   - ogólną ocenę rozwiązań;
   - weryfikację polityki zarządzania urządzeniami;
   - ocenę mechanizmów bezpieczeństwa;
   - analizę dostępów do urządzenia;
   - analizę routingu;
   - analizę i filtrowanie połączeń;
   - badanie redundancji rozwiązań.

4. Przegląd konfiguracji i oprogramowania zabezpieczającego obejmuje:
   - badanie luk systemów teleinformatycznych i aplikacji;
   - analizę zabezpieczeń stacji roboczych i nośników danych, w szczególności tych, na których przetwarzane są dane osobowe, weryfikacja procedur planowania aktualizacji systemów teleinformatycznych;
   - weryfikację ochrony przed oprogramowaniem szkodliwym, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania;
   - weryfikację zasad i procedur zarządzania historią zmian konfiguracji sprzętu lub oprogramowania.

5. Przegląd konfiguracji baz danych obejmuje:
- badanie luk baz danych;
- proces i metody autoryzacji;
- ocenę zarządzania uprawnieniami i logowaniem zdarzeń;
- ocenę zarządzania zmianami konfiguracyjnymi i aktualizacjami;
- ocenę konfiguracji systemu operacyjnego serwera;
- ocenę dostępności i ciągłości działania;
- analizę systemu zarządzania kopiami zapasowymi.

6. Badanie podatności sieci LAN za pomocą regularnie aktualizowanego automatycznego skanera bezpieczeństwa obejmuje:
- badanie luk systemów teleinformatycznych i aplikacji;
- badanie luk urządzeń sieciowych;
- badanie luk baz danych;
- badanie luk komputerów i notebooków;
- badanie luk serwerów;
- inwentaryzację otwartych portów;
- analizę bezpieczeństwa stosowanych protokołów;
- identyfikację podatności systemów i sieci na ataki typu: dos, ddos, sql, injection, sniffing, spoffing, xss, hijacking, backdoor, flooding, passwordguessing.

7. Badanie podatności styku sieci lokalnej z Internetem przeprowadzone jest z komputera lub innego urządzenia podłączonego do systemu informatycznego z zewnątrz (poprzez urządzenie łączące system informatyczny urzędu z Internetem), mające na celu zidentyfikowanie możliwości przeprowadzenia włamania z zewnątrz i obejmuje działania:
- inwentaryzacja otwartych portów;
- analizę bezpieczeństwa stosowanych protokołów;
- identyfikację podatności systemów i sieci na ataki typu: dos, ddos, sql, injection, sniffing, spoffing, xss, hijacking, backdoor, flooding, passwordguessing.

8. Badanie stanu ochrony fizycznej i technicznej. Weryfikacja procedur zarządzania systemami teleinformatycznymi obejmuje działania:
weryfikację procedur planowania aktualizacji systemów teleinformatycznych;
weryfikację ochrony przed oprogramowaniem szkodliwym, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania;
weryfikację zasad i procedur zarządzania historią zmian konfiguracji sprzętu lub oprogramowania;
- weryfikację zasad i procedur zarządzania kopiami zapasowymi;
- weryfikację zasad i procedur zabezpieczania nośników;
- weryfikację zasad i procedur kontroli dostępu do systemów teleinformatycznych;
- weryfikację zasad i procedur dostępu do systemów operacyjnych;
- weryfikację zasad i procedur dostępu do usług internetowych;
- weryfikację zasad i procedur zarządzania hasłami;
- weryfikację zabezpieczeń kryptograficznych;

- weryfikację kontroli eksploatowanego oprogramowania;
- weryfikację systemów monitorujących;
- weryfikację zasad i procedur rejestracji błędów;
- weryfikację zasad i procedur postępowania z urządzeniami przenośnymi, w szczególności tymi, na których przetwarzane są dane osobowe;
- weryfikację zasad i procedur związanych z użytkowaniem sprzętu poza siedzibą.
- weryfikację zasad i procedur bezpiecznego przekazywania sprzętu;
- weryfikację zasad i procedur niszczenia niepotrzebnych nośników;
- weryfikację zasad i procedur składowania danych elektronicznych;
- weryfikację zasad i procedur wykonywania kopii, obejmująca minimum: sposób wykonywania kopii bezpieczeństwa, zakres kopiowanych danych, przechowywanie kopii bezpieczeństwa oraz administracji kopiami i dostępu do kopii.

III. Audyt Legalności Oprogramowania:

1. Inwentaryzacja zainstalowanego na dyskach twardych oprogramowania (skanowanie wszystkich komputerów będących w posiadaniu Zleceniodawcy).

2. Inwentaryzacja dokumentacji licencyjnej przedstawionej przez Zleceniodawcę.

3. Weryfikacja zgodności zainstalowanego oprogramowania z posiadanymi licencjami.

4. Przygotowanie i przekazanie poufnego raportu wynikowego o stanie legalności oprogramowania po pierwszym skanowaniu:
a) w formie pisemnego dokumentu:
- opis procedury audytu;
- opis stanu zarządzania oprogramowaniem na dzień audytu;
- zalecenia naprawcze;
- wzory dokumentów:
  - metryka komputera;
  - porozumienie z pracownikiem;
  - wzór zarządzenia.
- zestawienia tabelaryczne:
  - szczegółowe raporty systemów operacyjnych OEM z kluczami instalacyjnymi;
  -zbiorcze zestawienie Systemów operacyjnych z podziałem na rodzaje licencji;
  - szczegółowy raport aplikacji Office OEM z kluczami instalacyjnymi;
  - zbiorcze zestawianie Pakietów Office z podziałem na rodzaje licencji.

b) w wersji elektronicznej na nośniku CD:
- kopia wersji pisemnej;
- zawierającego informacje o zainstalowanym oprogramowaniu na poszczególnych stacjach roboczych;
- wykaz zainstalowanego w firmie oprogramowania ze wskazaniem ścieżki dostępu poszczególnych instalacji.

5. Omówienie rozbieżności między zainstalowanym na komputerach oprogramowaniem, a posiadanymi licencjami, wykazanie ewentualnych braków w dokumentacji licencyjnej oraz wskazanie sposobów ich eliminacji.

6. Wskazanie najkorzystniejszych możliwości, uzupełnienia brakujących licencji.

7. Sporządzanie spisu oprogramowania do usunięcia lub uzupełnienia licencji.

8. Przekazanie do Microsoft dokumentu Effective License Positions (ELP).

9. Merytoryczna pomoc przy opracowaniu właściwych firmowych Zasad Zarządzania Oprogramowaniem oraz przekazanie wzorów dokumentów (porozumienie, metryka, zarządzenie).

10. Przygotowanie i przekazanie końcowego raportu wynikowego z przeprowadzonego audytu przed terminem zakończenia audytu.

11. Wystąpienie do firmy Microsoft z wnioskiem o nadanie Zleceniodawcy Certyfikatu „Microsoft Software Assets Management".

IV. Aktualizacja Polityki Bezpieczeństwa Danych Osobowych:

1. Analiza istniejącej Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym:
a) analiza dokumentu Polityki Bezpieczeństwa;
b) weryfikacja kompletności wymaganej dokumentacji;
c) analiza procedur obowiązujących w instytucji;
d) weryfikacja rejestru osób upoważnionych do przetwarzania danych osobowych, upoważnień oraz innych dokumentów (oświadczenia, karty uprawnień itp.).

2. Wizja lokalna poziomu zabezpieczeń:
a) Inwentaryzacja obszarów przetwarzania danych:
- analiza bezpieczeństwa fizycznego;
- analiza bezpieczeństwa organizacyjnego;
- analiza bezpieczeństwa technicznego (informatycznego);

b)Inwentaryzacja zbiorów danych i systemów, w których są przetwarzane dane:
- inwentaryzacja zbiorów danych (papierowa i elektroniczna);
- analiza zbiorów danych osobowych, w których przetwarzane są dane szczególnie chronione.

c) Inwentaryzacja środków technicznych i organizacyjnych stosowanych w celu zapewnienia poufności, integralności i rozliczalności przetwarzanych danych:
- weryfikacja pracy użytkowników w obszarach, w których przetwarzane są dane osobowe;
- weryfikacja sposobu przetwarzania danych osobowych;
- weryfikacja kontroli nad przepływem danych osobowych;

- weryfikacja przechowywania danych osobowych.

3. Zebranie informacji od Administratora Danych Osobowych, Administratora Bezpieczeństwa Informacji, Inspektora Bezpieczeństwa Teleinformatycznego, Administratora Systemu Sieci Teleinformatycznej dotyczących stosowanych praktyk i procedur:

a)nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazania osoby odpowiedzialnej za te czynności;
b)stosowania metod i środków uwierzytelnienia oraz procedur związanych z ich zarządzaniem i użytkowaniem;
c)rozpoczęcia, zawieszenia i zakończenia pracy użytkowników systemu;
d) tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
e)sposobu, miejsca i okresu przechowywania:

- elektronicznych nośników informacji zawierających dane osobowe;
- kopii zapasowych.

f)sposobu zabezpieczenia systemu informatycznego przed szkodliwą działalnością oprogramowania;
g)wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

4. Opracowanie i przekazanie Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym.

IV. Opracowanie raportu zawierającego wskazówki niezbędnych działań do spełnienia wymogów Krajowych Ram Interoperacyjności odnoszących się do Bezpieczeństwem Informacji.

V. Termin wykonania zamówienia: termin realizacji – 30 dni od daty podpisania umowy.

VI. Kryterium wyboru oferty: cena, doświadczenie, kwalifikacje wykonawcy

<u>Kryteria oceny ofert:</u>

70% - Cena.

25% - Doświadczenie polegające na przeprowadzeniu więcej niż 15 działań audytowych w jednostkach administracji publicznej w ciągu ostatnich 24 miesięcy:

- 15 i mniej działań audytowych (jednostek audytowanych) – 0 pkt

- 16 – 20 działań audytowych (jednostek audytowanych) - 5 pkt

- 21-30 działań audytowych (jednostek audytowanych) - 10 pkt

- powyżej 30 działań audytowych (jednostek audytowanych) – 25 pkt

5% - Posiadanie przez osoby bezpośrednio wykonujące audyt certyfikatów: Microsoft MCP, Microsoft MCSA:
- nie posiada – 0 pkt.,
- posiada – 5 pkt.

VII. Warunki udziału w postępowaniu oraz opis sposobu przygotowania oferty

Wymagania wobec Wykonawców/osób bezpośrednio realizujących przedmiot zamówienia:

- posiada uprawnienia Audytora Wiodącego ISO 27001:2013

Warunki udziału:

1. Wiedza i doświadczenie

Wykonawca lub Audytor bezpośrednio wykonujący zadanie audytowe zobowiązany jest wykazać, że w okresie ostatnich 24 miesięcy przed upływem terminu składania ofert, a jeśli okres prowadzenia działalności jest krótszy - w tym okresie, należycie wykonał co najmniej: 15 zamówień, polegających na wdrożeniu systemu bezpieczeństwa informatycznego lub przeprowadzeniu audytu systemu bezpieczeństwa informatycznego w jednostkach sektora publicznego, zgodnie z Rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych lub standardem ISO 27001.

2.Osoby zdolne do wykonania zamówienia:

Wykonawca zobowiązany jest wykazać, że dysponuje zespołem składającym się co najmniej z 2 osób, w tym audytora wiodącego legitymującego się niżej wymienionymi certyfikatami:

•Audytor Wiodący ISO 27001: 2013;
•Audytor wewnętrzny ISO 27001

Dodatkowo, pożądane:
•Microsoft MCP
•Microsoft MCSA

Dokumenty jakie winien przedłożyć Wykonawca:

1. Wykaz osób uczestniczących w wykonywaniu zamówienia wraz z potwierdzeniem niezbędnych kwalifikacji, uprawnień

2 .Wykaz wykonanych usług wykonanych w ciągu ostatnich 24 miesięcy.

3. Oświadczenia osób bezpośrednio wykonujących audyt o niekaralności.

4. W przypadku podpisywania dokumentów, przez osoby upoważnione/ pełnomocników, należy złożyć stosowne dokumenty potwierdzające upoważnienie/ pełnomocnictwo.

5. Szczegółowy harmonogram działań audytowych.

Niespełnienie warunków udziału w postępowaniu lub niezłożenie któregokolwiek z w/w dokumentów spowoduje odrzucenie oferty Wykonawcy.

VIII. Termin, miejsce i forma składania ofert

Ofertę w formie pisemnej należy przesłać na adres: Urząd Miejski w Giżycku, al. 1 Maja 14, 11-500 Giżycko w terminie do dnia **29 lipca 2016r. do godz.11:00.** Liczy się data wpływu oferty do Urzędu. Oferty złożone po terminie nie będą rozpatrywane i zostaną zwrócone bez otwierania.

Oferta powinna być oznaczona napisem: **„Oferta: Wykonanie Audytu Bezpieczeństwa Informacji w Urzędzie Miejskim w Giżycku"**

UWAGA! Zamawiający zastrzega sobie prawo do:

1) swobodnego wyboru ofert w ramach prowadzonego postępowania,
2) odwołania postępowania, unieważnienia go w całości lub w części w każdym czasie,
3) zamknięcia postępowania bez dokonania wyboru oferty oraz bez uzasadnienia,
4) zmiany terminów wyznaczonych w ogłoszeniu,
5) żądania dokumentów, szczegółowych informacji i wyjaśnień od Wykonawców na każdym etapie przetargu,
6) wyłącznej interpretacji zapisów ogłoszenia, jak również jego załączników.

Z up. Burmistrza
Arkadiusz Połojański
Sekretarz Gminy Miejskiej