S P E C Y F I K A C J A I S T O T N Y C H W A R U N K Ó W Z A M Ó W I E N I A

PRZETARG OFERTOWY

o szacunkowej wartości poniżej 14 000 euro

Sprawa nr: DOA-0410-8/JL/2011

Przedmiot zamówienia:

Przetarg ofertowy na audyt teleinformatyczny.

Zamawiający:

Powiatowy Urząd Pracy w Sochaczewie,
reprezentowany przez Dyrektora Powiatowego Urzędu Pracy
ulica Kusocińskiego 11
96 – 500 Sochaczew
www.pup.sochaczew.pl
e-mail: sekretariat@pup.sochaczew.pl

Sochaczew, 09 grudnia 2011 roku.

Postępowanie prowadzone z wyłączeniem procedur wynikających z ustawy – Prawo zamówień publicznych (art. 4, pkt 8 ustawy j/w)

Ogłoszenie o przetargu ofertowym na przeprowadzenia audytu teleinformatycznego.

Postępowanie prowadzone z wyłączeniem procedur wynikających z ustawy- Prawo Zamówień publicznych(art.4 pkt.8 ustawy j.w.)

Powiatowy Urząd Pracy w Sochaczewie ogłasza przetarg ofertowy na **: przeprowadzenie audytu teleinformatycznego ze szczególnym uwzględnieniem ich bezpieczeństwa** (na bazie zakresu prac audytowych poniżej)

Dane do sporządzenia wyceny:

Ilość stanowisk: 45

Ilość serwerów: 3

Ilość lokalizacji: 1

Termin realizacji: - **nieprzekraczalny do 30.12.2011r.**

Termin płatności: **- 14 dni**

Miejsce realizacji: **- Sochaczew ul. Kusocińskiego 11**

Osoba uprawniona do kontaktów z oferentami:

Jadwiga Libera tel. /046/ 862 24 55 wew. 141

Zamkniętą kopertę z ofertą oznaczoną –

„Przetarg ofertowy na audyt teleinformatyczny"

należy złożyć w siedzibie Zamawiającego przy ul. Kusocińskiego 11, 96-500 Sochaczew w Sekretariacie - pok. nr 45.

Termin składania ofert upływa dnia **16.12.2011 r. o godz. 10.00.**

Otwarcie ofert nastąpi w dniu **16.12.2011r. o godz. 10.30** w siedzibie Zamawiającego w pokoju 41.

Kryteria oceny ofert:

Najniższa cena

INSTRUKCJA DLA OFERENTÓW

1. Zakres zamówienia

1.1 Termin realizacji: - **nieprzekraczalny do 30.12.2011r.**

1.2 Termin płatności: **- 14 dni**

1.3 Przedmiot zamówienia – **przeprowadzenie audytu teleinformatycznego ze szczególnym uwzględnieniem ich bezpieczeństwa** (na bazie zakresu prac audytowych poniżej)

Dane do sporządzenia wyceny:

Ilość stanowisk: 45

Ilość serwerów: 3

Ilość lokalizacji: 1

2. Opis sposobu przygotowania ofert

2.1 Ofertę stanowi „formularz oferty" sporządzony do specyfikacji wraz z zaświadczeniami, oświadczeniami i dokumentami wymienionymi w niniejszej specyfikacji.

2.2 W przypadku, gdy Oferent jako załącznik dołączy kopie jakiegoś dokumentu, powyższa kopia winna być potwierdzona przez uprawomocnionego reprezentanta Oferenta.

2.3 Oferta winna być napisana w języku polskim, podpisana przez upoważnionego przedstawiciela Oferenta - przy czym podpis lub podpisy muszą być czytelne lub opisane pieczątkami imiennymi.

Również wszystkie załączniki do oferty, stanowiące oświadczenia Oferenta winny być podpisane. Upoważnienie do podpisania oferty winno być dołączone do oferty, o ile nie wynika z innych dokumentów załączonych przez Oferenta.

2.5 Oświadczenia lub zawiadomienia przekazane za pomocą teleksu, faksu uważa się za złożone w terminie, jeżeli ich treść dotarła do adresata przed upływem terminu i została niezwłocznie potwierdzona na piśmie przez przekazującego.

2.6 Zaleca się aby wszystkie strony zapisane (tylko zawierające treść) oferty były ponumerowane kolejnymi numerami, oraz wymaga aby wszystkie miejsca, w których Oferent naniósł zmiany w treści oferty, były parafowane przez osobę podpisującą ofertę.

2.7 Kopertę należy adresować na Zamawiającego z zaznaczeniem:

„Przetarg ofertowy na audyt teleinformatyczny"

oraz „Nie otwierać przed 16.12.2011 r. godz. 10.30 ".

2.8 Oferent może przed upływem terminu do składania ofert wprowadzić zmiany lub wycofać ofertę. Powiadomienie o wprowadzeniu zmian lub wycofaniu oferty winno mieć na kopercie oznaczenie „Zmiana" lub „ Wycofanie".

2.9 Oferent ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

2.10 Oświadczenia, wnioski, zawiadomienia oraz informacje przekazane za pomocą faksu uważa się za złożone w terminie, jeżeli ich treść dotarła do adresata przed upływem terminu i została niezwłocznie potwierdzona pismem. Zamawiający nie dopuszcza elektronicznej drogi porozumiewania się z Oferentem.

3. Dokumenty składające się na ofertę

3.1. Oferta musi zawierać następujące dokumenty i oświadczenia:

3.1.1 Aktualny odpis z właściwego rejestru lub aktualne zaświadczenie o wpisie do ewidencji gospodarczej, o profilu odpowiadającym przedmiotowi zamówienia, wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

3.1.2 Oświadczenie o spełnianiu warunków – z**ałącznik nr 2.**

3.1.3 Zaparafowaną propozycję umowy – z**ałącznik nr 3.**

3.1.4 Wypełniony formularz „Oferta cenowa" - z**ałącznik nr 1.**

3.1.5 Minimum trzy listy referencyjne z Urzędów Pracy na wykonanie audytu teleinformatycznego z ostatnich 2 lat.

3.1.7 Certyfikaty deklaracji zgodności S.K.W. urządzenia demagnetyzującego Mediaeraser Degausser MD103.

3.1.8 Poświadczenie aktualnej licencji na oprogramowanie do testów penetracyjnych.

4. Sposób udzielania wyjaśnień dotyczących niniejszej specyfikacji istotnych warunków zamówienia

4.1 Upoważnieni do bezpośredniego kontaktowania się z Oferentami jest:
Jadwiga Libera - w godz. 7.30 do 15.30 nr. tel. 46 864 24 55 w. 141

4.2 Oferent winien zapoznać się ze wszystkimi zapisami niniejszej specyfikacji istotnych warunków zamówienia. Zaleca się, aby oferent zdobył wszelkie informacje, które mogą być konieczne do przygotowania oferty oraz podpisania umowy. Oferent poniesie wszystkie koszty związane z przygotowaniem i złożeniem oferty.

5. Okres związania ofertą

5.1 Oferent pozostaje związany ofertą przez okres 30 dni od daty upływu terminu wyznaczonego na składanie ofert.

6. Miejsce i termin składania ofert

6.1 Ofertę należy złożyć w siedzibie Zamawiającego,
6.2 Termin składania ofert upływa dnia **16.12.2011r. do godziny 10.00**
6.3 Oferty otrzymane przez Zamawiającego po terminie podanym w pkt 6.2. zostaną zwrócone Oferentom bez otwierania.

7. Otwarcie i badanie ofert
7.1 Zamawiający otworzy oferty w dniu **16.12.2011r. o godzinie 10.30** w siedzibie Zamawiającego w pokoju 41. Otwarcie nastąpi w obecności przybyłych Oferentów.
7.2 Podczas otwarcia Zamawiający ogłosi nazwy(firmy) i adresy Oferentów oraz ceny ofert, warunki gwarancji, terminy płatności i inne składniki podlegające ocenie.
7.3 W toku dokonywania badania i oceny złożonych ofert Zamawiający może żądać udzielenia przez Oferentów wyjaśnień dotyczących treści złożonych przez nich ofert.

8. Kryteria oceny ofert i wyboru oferty najkorzystniejszej
8.1 Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującym kryterium- **najniższa cena**

9. Unieważnienie postępowania
Zamawiający zastrzega sobie możliwość unieważnienia niniejszego postępowania bez podawania przyczyn.

10. Informacja o formalnościach po wyborze oferty
Zamawiający poinformuje Wykonawcę, którego oferta zostanie wybrana jako najkorzystniejsza o miejscu i terminie zawarcia umowy.

Szczegółowy zakres zadania.

Kompleksowa usługa wykonania audyt systemów teleinformatycznych, ze szczególnym uwzględnieniem ich bezpieczeństwa oraz utylizacja Danych- kasowanie nośników w Powiatowym Urzędzie Pracy w Sochaczewie, składająca się z:

3.1 Audytu Systemów Teleinformatycznych.

3.1.1 Audyt bezpieczeństwa teleinformatycznego audyt systemów teleinformatycznych, ze szczególnym uwzględnieniem ich bezpieczeństwa **Audyt systemów teleinformatycznych** ma na celu ustalenie stanu bieżącego systemów teleinformatycznych wykorzystywanych przez Zamawiającego oraz wykrycie i ustalenie potencjalnych zagrożeń związanych z utratą lub nieautoryzowanym dostępem do informacji przetwarzanych, gromadzonych i przechowywanych w systemach teleinformatycznych, za pomocą metodologii zgodnej z dobrą praktyką według norm ISO 27001 i ISO 20000 oraz narzędzia do sprawdzania podatności Tenable Nessus.

Na audyt składać się będą:

Wyszczególnione poniżej działania i czynności:

(1) Weryfikacja procedur zarządzani systemami teleinformatycznymi.
(2) Weryfikacja procedur planowania aktualizacji systemów teleinformatycznych.
(3) Weryfikacja ochrony przed oprogramowaniem szkodliwym, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania.
(4) Weryfikacja zasad i procedur zarządzania historią zmian konfiguracji sprzętu lub oprogramowania.
(5) Weryfikacja zasad i procedur zarządzania kopiami zapasowymi.
(6) Weryfikacja zasad i procedur zabezpieczania nośników.
(7) Weryfikacja zasad i procedur kontroli dostępu do systemów teleinformatycznych.
(8) Weryfikacja zasad odpowiedzialności użytkowników**.**
(9) Weryfikacja zasad i procedur dostępu do systemów operacyjnych.
(10) Weryfikacja zasad i procedur dostępu do usług internetowych.
(11) Weryfikacja zasad i procedur zarządzania hasłami.
(12) Weryfikacja zabezpieczeń kryptograficznych.
(13) Weryfikacja kontroli eksploatowanego oprogramowania.
(14) Weryfikacja zabezpieczeń komputerów przenośnych.
(15) Weryfikacja bezpieczeństwa sieci LAN, WAN.
(16) Weryfikacja zasad i procedur użytkowania Internetu.
(17) Weryfikacja systemów monitorujących.
(18) Weryfikacja zasad i procedur rejestracji błędów.
(19) Weryfikacja metod autoryzacji na stacjach roboczych.
(20) Analiza zabezpieczeń stacji roboczych i nośników danych, w szczególności tych, na których przetwarzane są dane osobowe.
(21) Weryfikacja zasad i procedur postępowania z urządzeniami przenośnymi, w szczególności tymi, na których przetwarzane są dane osobowe.
(22) Weryfikacja zasad i procedur związanych z użytkowaniem sprzętu poza siedzibą.

(23) Weryfikacja zasad i procedur bezpiecznego przekazywanie sprzętu.
(24) Weryfikacja zasad i procedur niszczenie niepotrzebnych nośników.
(25) Weryfikacja zasad i procedur składowania danych elektronicznych.
(26) Weryfikacja zasad i procedur wykonywania kopii, obejmująca minimum: sposób wykonywania kopii bezpieczeństwa, zakres kopiowanych danych, przechowywanie kopii bezpieczeństwa oraz administracji kopiami i dostępu do kopii.
(27) Analiza konfiguracji wykorzystywanych serwerów, stacji roboczych i aplikacji, obejmująca minimum:
a) Techniczną ocenę rozwiązania.
b) Politykę zarządzania.
c) Proces i metody autoryzacji.
d) Zarządzanie uprawnieniami i logowanie zdarzeń.
e) Zarządzanie zmianami konfiguracyjnymi i aktualizacjami.
f) Ocenę konfiguracji systemu operacyjnego.
g) Dostępność i ciągłość działania.
h) Analizę systemu zarządzania kopiami zapasowymi.
i) Analizę bezpieczeństwa funkcji i protokołów specyficznych dla aplikacji /serwera.
(28) Analiza konfiguracji aktywnych urządzeń sieciowych, obejmująca minimum:
a) Ogólną ocenę rozwiązania.
b) Politykę zarządzania.
c) Ocenę mechanizmów bezpieczeństwa.
d) Analizę dostępów do urządzenia.
e) Routing.
f) Analizę i filtrowanie połączeń.
g) Redundancję rozwiązań.

2) Opisane poniżej testy penetracyjne:

(1) Przeprowadzone 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.

(2) Przeprowadzone z komputera lub innego urządzenia podłączonego do systemu informatycznego z wewnątrz w celu zidentyfikowania możliwości przeprowadzenia włamania z wewnątrz urzędu.

(3) Testy penetracyjne muszą obejmować minimum następujące obszary:
a) Badanie luk systemów teleinformatycznych i aplikacji.
b) Badanie luk urządzeń sieciowych.
c) Badanie luk baz danych.
d) Badanie luk komputerów i notebooków.
e) Badanie luk serwerów.

(4) Przeprowadzone testy penetracyjne muszą umożliwiać minimum:
a) Inwentaryzację otwartych portów.
b) Analizę bezpieczeństwa stosowanych protokołów.
c) Identyfikację podatności systemów i sieci na ataki typu: DoS, DDoS, SQL, Injection, Sniffing, Spoffing, XSS, Hijacking, Backdoor, Flooding, Password

Guessing, oraz ewentualne inne, uznane przez Wykonawcę za wskazane do przeprowadzenia.
3) Skanowanie wszystkich aktywnych urządzeń działających w sieci komputerowej LAN i WAN Zamawiającego, w tym: routerów, zapór ogniowych, przełączników, serwerów, komputerów stacjonarnych i komputerów mobilnych oraz oprogramowania na nich zainstalowanego, mające na celu wykrycie i zdiagnozowanie występujących luk zabezpieczeń i podatności na atak w tych urządzeniach oraz błędów w konfiguracji urządzeń i oprogramowania zmniejszających poziom bezpieczeństwa systemów. Skanowanie wykonane zostanie zgodnie z poniższymi wytycznymi:
(1) Zastosowane narzędzia do skanowania podatności umożliwią przeprowadzenie analizy ryzyka systemów IT na poziomie technologicznym.
(2) Zostanie zweryfikowana zgodność na poziomie technologicznym konfiguracji systemów operacyjnych komputerów i serwerów z wytycznymi wynikającymi z polityki bezpieczeństwa.
(3) W procesie skanowania zostanie wykorzystane urządzenie specjalizowane i dedykowane dla przeprowadzenia takiego procesu.
(4) Proces skanowania nie może powodować braku możliwości wykonywania przez Zamawiającego bieżących zadań wynikających z mocy prawa.
(5) Przeskanowane zostanie także oprogramowanie pakietów biurowych oraz systemu poczty elektronicznej zainstalowane na stacjach roboczych.
(6) W procesie skanowania wykorzystywane będą najnowsze bazy podatności publikowane w serwisach CVE oraz producentów sprzętu i systemów operacyjnych.
(7) W celu wykrycia luk zabezpieczeń i podatności na atak nie będą przeprowadzane jakiekolwiek działania o skutkach destrukcyjnych. Stwierdzona luka lub podatność
na atak będzie potwierdzana autentykacją i logowaniem uzyskanego dostępu.
(8) Skanowanie urządzeń musi odbyć się bez instalacji jakiegokolwiek dodatkowego oprogramowania na badanych urządzeniach.
(9) Po przeskanowaniu sieci zostanie sporządzony szczegółowy raport dotyczący wykrytych podatności.
(10) Do każdej wykrytej podatności lub błędnej konfiguracji zostanie przygotowana instrukcja w jaki sposób ją wyeliminować.
(11) Po skanowaniu audytowym odbędzie się 1 zdalne skanowania kontrolne w odstępie 3 miesięcy, a po jego wykonaniu zostanie sporządzony raport trendu podatności i poziomu ryzyka systemów.

Audyt zakończy się sporządzeniem przez Wykonawcę raportu pokontrolnego, opracowanego na podstawie dobrych praktyk wskazanych w normach ISO 27001 i ISO 20000, zawierającego:
1) Opis i zakres przeprowadzonych prac audytowych.
2) Analizę informacji zebranych podczas audytów.
3) Wnioski i zalecenia audytora.
4) Rozwiązania wykrytych i zidentyfikowanych zagrożeń występujących w ramach zbadanych obszarów.
5) Ocenę poziomu bezpieczeństwa danych i systemów teleinformatycznych.

6) Interpretację wyników przeprowadzonego audytu bezpieczeństwa przetwarzania danych, ze szczególnym uwzględnieniem danych osobowych w kontekście bezpieczeństwa przetwarzania danych w systemach teleinformatycznych.
7) Analizę wyników testów penetracyjnych pod kątem oceny zagrożenia integralności systemu oraz możliwości dostępu do danych przez osoby nieupoważnione.
8) Informacje na temat wykrytych luk w mechanizmach bezpieczeństwa.
9) Zalecenia dotyczące zabezpieczenia systemów teleinformatycznych i wyznaczenie kierunków dalszego rozwoju systemów zabezpieczających.
10) Raport z audytu zgodny będzie z:
(1) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm).
(2) Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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).

Wszystkie dokumenty związane z przeprowadzonym audytem Wykonawca dostarczy Zamawiającemu w postaci wydruku w dwóch egzemplarzach i w postaci elektronicznej na optycznym nośniku danych. Wykonawca pisemnie zobowiąże się, że dokumenty te będzie traktował jako poufne i nie przekaże ani nie udostępni ich nikomu bez pisemnej zgody Zamawiającego, z wyłączeniem organów występujących o to z mocy prawa po uprzednim powiadomieniu o tym wystąpieniu Zamawiającego. Usługodawca przeprowadzi audyt w oparciu o posiadaną aktualną licencję na oprogramowanie do testów penetracyjnych.

5. Wydanie Certyfikatu potwierdzającego wykonanie Audytu Systemów Teleinformatycznych;

I. Utylizacja Danych- kasowanie nośników Mediaeraser Degausser MD103 (certyfikowanym przez Służbę Kontrwywiadu Wojskowego)

1. **Fizyczna utylizacja nośników polega** na całkowitym wykasowaniu zawartych na nośniku jakichkolwiek danych za pomocą Utylizatora Danych - Degaussera. (zgodnie z ustawą „ElektroG" - Ustawa o wprowadzeniu do obrotu, zwrocie i przyjaznym dla środowiska usuwaniu odpadów urządzeń elektrycznych i elektronicznych z dnia 24.03.2006r)
2. **Liczba dysków twardych około 10 sztuk, taśm około 5 szt I dyskietki**
3. **Specyfikacja techniczna urządzenia:**
   - Zasilanie: 230V AC 50/60 Hz,
   - Czas operacji: kasowanie: 40 s/nośnik,
   - Generowane pole magnetyczne: 9 000 Gaussów,
   - System odmagnesowywania:
     Pojemnościowy system wyładowujący,
   - Rodzaje nośników: dyski twarde 2,5', 3,5', taśmy DLT, LTO, 3490 i inne,
   - Posiada znak CE.

4. **Kasowanie zakończy się sporządzeniem przez Wykonawcę raportu oraz certyfikatem**

ZAMAWIAJĄCY WYKONAWCA