POWIATOWY URZĄD PRACY
17-300 SIEMIATYCZE
ul. Legionów Piłsudskiego 3
tel. 85 656 60 13, fax 85 656 60 16
NIP 5441175642 REG. 050869816

Siemiatycze, 09.08.2017

miejscowość i data

pieczęć zamawiającego

Zapytanie ofertowe

I. Nazwa (firma) i adres zamawiającego:

Nazwa Zamawiającego:	Powiatowy Urząd Pracy w Siemiatyczach
Adres Zamawiającego:	Legionów Piłsudskiego 3
Kod Miejscowość:	17-300 Siemiatycze
Telefon:	85 656 60 13
Faks:	85 656 60 16
Adres strony internetowej:	http://siemiatycze.praca.gov.pl
Adres poczty elektronicznej:	bisi@praca.gov.pl
Godziny urzędowania:	PON: 8^{00}-16^{00} WT-PT : 7^{30}-15^{30}

II. Tryb udzielania zamówienia.

Postępowanie nie podlega przepisom ustawy Prawo zamówień publicznych zgodnie z art. 4 pkt 8 ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (Dz. U. 2015r. poz. 2164 z późn. zm.) ze względu na wartość zamówienia oszacowana poniżej kwoty 30 000 euro i jest prowadzona w oparciu o uregulowania wewnętrzne obowiązujące u Zamawiającego.

III. Opis przedmiotu zamówienia.

Usługa winna być wykonana zgodnie z wymaganiami Ustawy z dnia 29.08.1997 r. o ochronie danych osobowych (Dz.U.2016 r., poz. 922 z późn. zm.) w oparciu o wymagania normy PN ISO/IEC 27001:2014-12 i Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 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.2004.100.1024) oraz zgodnie z wymaganiami ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. 2017 r., Nr 64, poz. 570) i 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.

Zakres usługi:

BEZPIECZEŃSTWO INFORMACJI

1. **Przygotowanie do audytu:**
   a) określenie celów audytu;
   b) uzgodnienie zakresu;

c) określenie odpowiedzialności;
d) identyfikacja działań i procesów.

2. **Weryfikacja zgodności z KRI dokumentacji odnoszącej się do:**
   a) organizacji bezpieczeństwa informacji;
   b) zarządzania aktywami;
   c) bezpieczeństwa zasobów ludzkich;
   d) bezpieczeństwa fizycznego i środowiskowego;
   e) zarządzania systemami i sieciami;
   f) kontroli dostępu;
   g) pozyskiwania, rozwoju i utrzymania systemów informatycznych;
   h) zarządzania incydentami bezpieczeństwa;
   i) zarządzania ciągłością działania;
   j) zgodności z regulacjami.

3. **Testy Penetracyjne:**
   a) przegląd konfiguracji stacji roboczych;
   b) przegląd konfiguracji serwerów;
   c) przegląd konfiguracji urządzeń sieciowych;
   d) przegląd konfiguracji oprogramowania zabezpieczającego;
   e) przegląd konfiguracji baz danych;
   f) badanie podatności z sieci LAN za pomocą automatycznego skanera bezpieczeństwa;
   g) badanie podatności sieci lokalnej z Internetem;
   h) badanie stanu ochrony fizycznej i technicznej.

4. **Przygotowanie raportu z audytu zawierającego:**
   a) cele audytu;
   b) zakres audytu;
   c) ustalenia dokonane podczas audytu;
   d) wskazówki niezbędnych działań do spełnienia wymogów Krajowych Ram Interoperacyjności odnoszących się do Bezpieczeństwem Informacji.

OCHRONA DANYCH OSOBOWYCH

1. Aktualizacja Polityki Bezpieczeństwa Danych Osobowych:
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.)

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.

Zebranie informacji od ADO, ABI, ASI, LABI 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.

Opracowanie i przekazanie kompletnej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji do zaimplementowania u zamawiającego wg aktualnego stanu prawnego oraz wymagań normy PN ISO/IEC 27001:2014-12: Polityka Bezpieczeństwa, Instrukcja Zarządzania Systemem Informatycznym wraz ze wszystkimi niezbędnymi procedurami uzupełniającymi oraz analizą ryzyka. Opracowana dokumentacja ma zapewnić możliwość zaimplementowania zmian określonych w Rozporządzeniu ogólnym o ochronie danych osobowych „RODO".

LEGALNOŚĆ OPROGRAMOWANIA

Legalność oprogramowania

1. Pełna 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. Wyszukanie i wykazanie plików multimedialnych (muzycznych, filmów) oraz „CRACK-ÓW".
5. Przygotowanie i przekazanie poufnego raportu wynikowego o stanie legalności oprogramowania po pierwszym skanowaniu w ciągu 14 dni od dnia rozpoczęcia audytu:
    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 (prezesa, dyrektora).
        - Zestawienia tabelaryczne
            - Szczegółowe raport 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.
            - Zbiorcze zestawienie aplikacji (opcjonalnie zbiorcze zestawienie wskazanego typu oprogramowania np. CAD, Graficzne inne).
    b) W wersji elektronicznej na nośniku CD;
        - Kopia wersji pisemnej.
        - Zawierającego informacje o zainstalowanym oprogramowaniu i innych plikach (MP3, gry, filmy, itd.) znajdujących się na poszczególnych stacjach roboczych.
        - Wykaz zainstalowanego w firmie oprogramowania ze wskazaniem ścieżki dostępu poszczególnych instalacji.

6. Omówienie rozbieżności między zainstalowanym na komputerach oprogramowaniem, a posiadanymi licencjami, wykazanie ewentualnych braków w dokumentacji licencyjnej oraz wskazanie sposobów ich eliminacji.
7. Wskazanie najkorzystniejszych możliwości, uzupełnienia brakujących licencji.
8. Sporządzanie spisu oprogramowania do usunięcia lub uzupełnienia licencji.
9. Przekazanie do Microsoft dokumentu Effective License Positions (ELP).
10. Merytoryczna pomoc przy opracowaniu właściwych firmowych Zasad Zarządzania Oprogramowaniem oraz przekazanie wzorów dokumentów (porozumienie, metryka, zarządzenie).
11. Ponowne skanowanie komputerów, weryfikacja dokumentacji i wdrożonych zasad zarządzania oprogramowaniem.
12. Przygotowanie i przekazanie końcowego raportu wynikowego z przeprowadzonego audytu przed dniem zakończenia audytu.
13. Wystąpienie do firmy Microsoft z wnioskiem o nadanie Zleceniodawcy Certyfikatu „Microsoft Software Assets Management".
14. Nadanie firmie Certyfikatu potwierdzającego uzyskanie zgodności z licencjami na pozostałe oprogramowanie i wdrożenie zasad zarządzania oprogramowaniem.

Opracowanie Polityki Zarządzania Oprogramowaniem

1. Opracowanie i opisanie Polityki Zarządzania Oprogramowaniem oraz sporządzenie dokumentu wprowadzającego te zasady w życie. Polityka ta obejmuje między innymi:
   a. zasady korzystania z oprogramowania przez pracowników w sposób zgodny z prawem,
   b. zasady instalacji oprogramowania,
   c. bieżące zarządzanie rejestrem licencji i instalacji,
   d. zasady nabywania oprogramowania,
   e. właściwe przechowywanie dokumentacji licencyjnej.

Uporządkowanie dokumentacji licencyjnej i wdrożenie Polityki Zarządzania Oprogramowaniem

1. Sporządzenie rejestru posiadanych licencji i instalacji w formacie xls lub w AuditPro, (jeśli Zleceniodawca zakupił licencje na ten system).

2. Segregacja dowodów licencyjnych (faktury zakupu, oryginalne nośniki, certyfikaty autentyczności, umowy licencyjne).
3. Stworzenie kompletów dokumentacji licencyjnej do całości oprogramowania zainstalowanego na poszczególnych stacjach roboczych.
4. Przygotowanie i wykonanie metryk komputerów.
5. Przygotowanie i wdrożenie porozumień z pracownikami:
   a) regulujących prawa i obowiązki pracowników w zakresie korzystania z oprogramowania,
   b) regulujących kwestie odpowiedzialności pracowników w przypadku naruszania praw autorskich.

Weryfikacja i porządkowanie zainstalowanego oprogramowania

1. Sprawdzenie zainstalowanego oprogramowania na poszczególnych komputerach z rejestrem licencji i metryką komputera.
2. Usunięcie nielegalnego oprogramowania z komputerów, na które Zleceniodawca nie posiada licencji oraz innych „utworów" chronionych prawem autorskim (pliki muzyczne, gry, filmy).
3. Zainstalowanie lub przeinstalowanie i konfiguracja oprogramowania, jeżeli wersje aktualnie zainstalowane nie odpowiadają posiadanym przez Zleceniodawcę licencjom.

IV. Termin wykonania zamówienia.

17.11.2017r.

V. Warunki udziału w postępowaniu.

W postępowaniu może wziąć udział Wykonawca, który:
1. Zrealizował przynajmniej.
   a) 10 audytów dotyczących ochrony danych osobowych w Urzędach Pracy w ciągu ostatnich 5 lat.
   b) 10 audytów teleinformatycznych w Urzędach Pracy w ciągu ostatnich 5 lat.
   c) 10 audytów informatycznych w Urzędach Pracy w ciągu ostatnich 5 lat.
2. Jest w stanie udokumentować współpracę informatyczną z Urzędami Pracy (dobre praktyki).
3. Dysponuje osobami zdolnymi zrealizować zamówienie **w ramach umowy o pracę:**
   a) audytora posiadającego certyfikat audytora wiodącego ISO/IEC 27001:2013.
   b) audytora posiadającego certyfikat audytora wewnętrznego ISO/IEC 27001:2005.
   c) audytora z wykształceniem z dziedziny ochrony danych osobowych.
   d) audytora wewnętrznego posiadającego certyfikat ISO 22301 (zarządzanie

ciągłością działania).

e) audytora wewnętrznego posiadającego certyfikat ISO 31000 (zarządzanie ryzykiem).
f) audytora wewnętrznego posiadającego certyfikat ISO 9001:2015 (zarządzanie jakością).
g) audytora wewnętrznego posiadającego certyfikat ISO 20000 (zarządzanie usługami).

4. Uczestniczy w programie Microsoft Software Asset Management (posiada certyfikat potwierdzający uczestnictwo w programie).
5. Posiada audytora, który zna zasady licencjonowania produktów i usług Microsoft, potwierdzone certyfikatami Microsoft Certificate of Excellence z zakresu Technology Specjalist.
6. Posiada audytora, który przeszedł szkolenie z zakresu funkcjonowania Administratora Bezpieczeństwa Informacji po 1 stycznia 2015 r.
7. **Posiada audytora, który jest pełnoprawnym członkiem Stowarzyszenia Administratora Bezpieczeństwa Informacji w Warszawie.**
8. Posiada audytora, który przeszedł szkolenie w zakresie kierunków zmian w systemie ochrony danych osobowych wobec wejścia w życie ogólnego rozporządzenia o ochronie danych osobowych do czerwca 2016 r.
9. Prowadząca działalność w zakresie, którego dotyczy przedmiot zamówienia przez okres co najmniej 4 lat przed dniem złożenia oferty.

Na potwierdzenie spełnienia warunków należy złożyć wykaz osób i dokumenty potwierdzające posiadanie w/w certyfikatów.

Podczas realizacji usługi w siedzibie zamawiającego Wykonawca powinien zapewnić uczestnictwo osób spełniających w/w wymagania wykazane w przedstawionej ofercie.

Zamawiający zastrzega sobie możliwość weryfikacji uprawnień osób realizujących usługę.

W ramach realizacji usługi Wykonawca zobowiązany jest do:
- przeprowadzenia usługi zgodnie z przedstawionym zakresem prac,
- oferta cenowa powinna zawierać całkowity koszt przeprowadzenia usługi.

VI. Wykaz dokumentów.

Na ofertę składają się następujące dokumenty i załączniki:

1. Formularz ofertowy - wypełniony i podpisany przez Wykonawcę.
2. Wykaz wykonanych audytów z danych osobowych, informatycznych, teleinformatycznych.

VII. Warunki płatności.

14 dni od daty otrzymania faktury.

VIII. Informacja o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń lub dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z Wykonawcami.

Ofertę na formularzu ofertowym wraz z załącznikami należy przesłać do dnia 25-08-2017 roku pocztą na adres Zamawiającego, faksem na numer 85 656 60 16 , na adres e-mail: bisi@praca.gov.pl lub złożyć osobiście w siedzibie Zamawiającego (sekretariat – pok. 3). Wykonawca jest związany złożoną ofertą przez okres 30 dni od dnia upływu terminu składania ofert.

IX. Informacje uzupełniające.

a) Zamawiający udzieli zamówienia Oferentowi, którego oferta spełni wymagania określone w niniejszym zapytaniu oraz zostanie uznana za najkorzystniejszą.
b) Zamawiający z wybranym Wykonawcą zawrze umowę niezwłocznie po przekazaniu zawiadomienia o wyborze oferty.

Konrad Pawluk

(podpis osoby prowadzącej postępowanie)

Konrad Pawluk

Zatwierdzam 09.08.2017

DYREKTOR
Powiatowego Urzędu Pracy
w Siemiatyczach
mgr Robert Maksimiuk