Załącznik do

zapytania ofertowego

Usługa winna być wykonana zgodnie z wymaganiami Ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2016r. poz. 922 ze zm.) i 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. z 2004r. Nr 100 poz. 1024) oraz zgodnie z wymaganiami ustawy z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2017r. 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 (Dz. U. z 2016r. poz. 113).

Usługę powinien wykonać podmiot, który:

1. Zrealizował przynajmniej
2. 5 audytów bezpieczeństwa informacji w Urzędach Pracy w ciągu ostatnich 5 lat.
3. 5 audytów teleinformatycznych w Urzędach Pracy w ciągu ostatnich 5 lat.
4. 5 audytów informatycznych w Urzędach Pracy w ciągu ostatnich 5 lat .
5. Dysponuje osobami zdolnymi zrealizować zamówienie w ramach umowy o pracę:
6. minimum 4 audytorów posiadających certyfikat audytora wiodącego ISO/IEC 27001:2013
7. minimum 2 audytorów posiadającym certyfikat audytora wewnętrznego ISO/IEC 27001:2005,
8. minimum 1 audytora z wykształceniem z dziedziny ochrony danych osobowych.
9. minimum 1 audytora wewnętrznego posiadającego certyfikat ISO 22301

(zarządzanie ciągłością działania)

1. minimum 2 audytorów wewnętrznych posiadających certyfikat ISO 31000

(zarządzanie ryzykiem)

1. minimum 2 audytorów wewnętrznych posiadających certyfikat ISO 27005

(zarządzanie ryzykiem)

1. minimum 2 audytorów wewnętrznych posiadających certyfikat ISO 20000
2. Uczestniczy w programie Microsoft Software Asset Management (posiada aktualny certyfikat potwierdzający uczestnictwo w programie).
3. Posiada przynajmniej 3 audytorów , którzy znają zasady licencjonowania produktów i usług Microsoft, potwierdzone certyfikatami Microsoft Certificate of Excellence z zakresu Technology Specjalist.
4. Prowadzi działalność w zakresie, którego dotyczy zapytanie cenowe przez okres co najmniej 5 lat przed dniem złożenia oferty.
5. Posiada umiejętności do jego wykonania w zwirtualizowanym środowisku serwerowym opisanym na początku dokumentu.

W ramach usługi „Audytu Bezpieczeństwa Informacji” ma być przeprowadzona:

**I.** **Weryfikacja spójności, kompletności i zgodności z przepisami prawa oraz Krajowymi Ramami Interoperacyjności 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.

**II. 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.

**III. Aktualizacja Polityki Bezpieczeństwa:**

**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 ADO i ABI 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.

**IV. Uporządkowanie dokumentacji licencyjnej i aktualizacja Polityki Zarządzania Oprogramowaniem.**

1. Sporządzenie rejestru posiadanych licencji i instalacji w formacie xls
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:
6. regulujących prawa i obowiązki pracowników w zakresie korzystania z oprogramowania,
7. regulujących kwestie odpowiedzialności pracowników w przypadku naruszania praw autorskich.
8. Aktualizacja Polityki Zarzadzania Oprogramowaniem.

**V. Audyt legalności 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. Przygotowanie i przekazanie poufnego raportu wynikowego o stanie legalności oprogramowania po pierwszym skanowaniu w ciągu 14 dni od dnia rozpoczęcia audytu:
   1. 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)
   2. 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.
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. Ponowne skanowanie komputerów, weryfikacja dokumentacji i wdrożonych zasad zarządzania oprogramowaniem.
11. Przygotowanie i przekazanie końcowego raportu wynikowego z przeprowadzonego audytu przed dniem zakończenia audytu.
12. Wystąpienie do firmy Microsoft z wnioskiem o nadanie Zleceniodawcy Certyfikatu „Microsoft Software Assets Management”.
13. Nadanie firmie Certyfikatu Firmy potwierdzającego uzyskanie zgodności z licencjami na pozostałe oprogramowanie i wdrożenie zasad zarządzania oprogramowaniem.

**VI. Opracowanie raportu zawierającego cele, zakres i ustalenia dokonane podczas audytu.**

**VII. Szkolenie pracowników z zakresu Polityki Bezpieczeństwa przeprowadzone w siedzibie tutejszego Urzędu (2 grupy).**

**VIII. Okres gwarancji**: doradztwo w ramach wykonanej usługi przez okres 12 miesięcy.