Załącznik nr 1 do zapytania ofertowego nr DKA.AM.2321.48.2017

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Zakres i przedmiot audytu obejmuje ocenę zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji, w tym przetwarzania danych osobowych w Regionalnym Ośrodku Polityki Społecznej w Lublinie z obowiązującymi aktami prawnymi w szczególności:

1. z wymogami § 20 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 2016 r., poz. 113 z późn. zm.),
2. zapisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 z późn. zm.),
3. normami bezpieczeństwa.

Liczba pracowników: 94
Liczba lokalizacji: 1
Liczba serwerów: 3
Liczba stacji roboczych: 81

Szczegółowy zakres audytu:

1. Przeprowadzenie audytu bezpieczeństwa informacji we wszystkich obszarach funkcjonowania ROPS w Lublinie.
   a) Audyt organizacyjny obejmujący między innymi:
      - regulacje w obszarze zarządzania bezpieczeństwem informacji,
      - odpowiedzialność za bezpieczeństwo informacji i koordynację prac związanych z zarządzaniem bezpieczeństwem informacji,
      - dokumentację, w tym z zakresu ochrony danych osobowych,
      - przeprowadzenie wywiadów z wybranymi pracownikami.
   b) Audyt fizyczny i środowiskowy w tym:
      - weryfikacja granic obszaru bezpiecznego,

- weryfikacja zabezpieczeń wejścia/wyjścia,
- weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń,
- weryfikacja bezpieczeństwa okablowania strukturalnego,
- weryfikacja systemów chłodzenia,
- weryfikacja systemów alarmowych.

c) Audyt teleinformatyczny z uwzględnieniem
- przeprowadzenia testów penetracyjnych systemu informatycznego wewnętrznie i zewnętrznie, określenie luk, wskazanie rozwiązań naprawczych, opracowanie raportu,
- weryfikacji istniejących procedur zarządzania systemami teleinformatycznymi,
- przeglądu zasobów informatycznych oraz stosowanych rozwiązań pod kątem utrzymania ciągłości działania,
- weryfikacji ochrony przed oprogramowaniem szkodliwym,
- weryfikacji procedur zarządzania kopiami zapasowymi,
- weryfikacji procedur związanych z rejestracją błędów,
- weryfikacji procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania,
- weryfikacji zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe,
- weryfikacji haseł (ich stosowanie, przyjęta polityka ich tworzenia oraz zmiany, mechanizmy ich przechowywania),
- analizy i oceny mechanizmów zarządzania aktualizacjami,

d) Audyt ochrony danych osobowych obejmujący:
- analizę formalno – prawną procesów i zbiorów, w których przetwarzane są dane osobowe, prowadzonych w sposób tradycyjny oraz z wykorzystaniem systemów informatycznych,
- przegląd zgodności przetwarzania danych osobowych z wymaganiami Ustawy,
- przegląd istniejących regulacji wewnętrznych odnośnie bezpieczeństwa przetwarzania danych osobowych,
- przegląd aktualnie wykorzystywanych dokumentów mających związek z ochroną danych osobowych,
- identyfikację zbiorów potencjalnie podlegających rejestracji.

e) Audyt legalności oprogramowania polegający na:

- inwentaryzacji oprogramowania wykorzystywanego w Ośrodku i dokumentacji licencyjnej,

f) Analizę szacowania ryzyka uwzględniającą:

- inwentaryzację aktywów podlegających szacowaniu ryzyka,
- określenie zagrożeń dla wyznaczonych aktywów,
- oszacowanie ryzyka pod kątem skutków naruszenia bezpieczeństwa informacji.

2. Wykonawca sporządzi sprawozdanie z audytu, które będzie zawierać:

a) Szczegółowy opis i ocenę stanu wszystkich obszarów podlegających audytowi.

b) Wykaz wszystkich problemów oraz wynikających z tego ryzyk wraz z oceną ryzyka wystąpienia wykrytych zagrożeń.

c) Zobrazowanie połączeń logicznych, sieci lokalnej oraz styku sieci lokalnej z siecią Internet, z uwzględnieniem wszystkich urządzeń ich adresacji i działających usług, używanych portów i protokołów.

d) Szczegółową, elektroniczną inwentaryzację sprzętu i oprogramowania działającego w infrastrukturze informatycznej Zamawiającego.

e) Zalecenia dotyczące sposobów, metod i środków usunięcia stwierdzonych problemów, nieprawidłowości, podatności i ryzyk. Lista poprawek do zainstalowania oraz szczegółowy opis zalecanych zmian konfiguracji.

f) Przygotowaną przez Wykonawcę aktualizację i uzupełnienie zestawu dokumentów Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym zgodną z aktualnie obowiązującymi aktami prawnymi. Dokumenty te Wykonawca przygotuje w porozumieniu z Zamawiającym, uwzględniając specyfikę działania i organizację pracy Zamawiającego.

Wszystkie dokumenty związane z przeprowadzonym audytem Wykonawca dostarczy Zamawiającemu w postaci wydruku w dwóch egzemplarzach i w postaci elektronicznej.

Wykonawca pisemnie zobowiąże się, że dokumenty te będzie traktował jako poufne i nie przekaże ani nie udostępni ich nikomu bez pisemnej zgody Zamawiającego.

Wykonawca, z dniem zatwierdzenia przez Zamawiającego sprawozdania z audytu, przeniesie na Zamawiającego autorskie prawa majątkowe do sprawozdania z audytu na polach eksploatacji, obejmujących:

a) odtwarzanie,

b) utrwalanie i trwałe zwielokrotnianie całości lub części utworu, wszystkimi znanymi w chwili zawierania Umowy technikami, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową,

c) przekazywanie,

d) przechowywanie,

e) wyświetlanie,

f) wprowadzanie do pamięci komputera wraz z prawem do dokonywania modyfikacji,

g) tłumaczenie,

h) przystosowywanie ,

i) zmiany układu lub jakiekolwiek inne zmiany.