Oświęcim, dnia 29.11.2017r.

Powiatowy Urząd Pracy w Oświęcimiu
ul. Wyspiańskiego 10
32 – 602 Oświęcim
tel.: (033) 844-41-44 wew. 1210
fax.: (033) 844-41-44 wew. 3212

INFORMUJE
o planowanej realizacji kompleksowego projektu z zakresu bezpieczeństwa informacji w Powiatowym Urzędzie Pracy w Oświęcimiu (w tym w Filii PUP w Kętach)

(postępowanie prowadzone zgodnie z art. 4 pkt 8 ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych. Tekst jed. z 2017r., poz. 1579)

Wszystkich zainteresowanych zapraszamy do złożenia oferty. Oferty można składać osobiście w siedzibie urzędu (dziennik podawczy – parter) lub przesłać pocztą na adres:
Powiatowy Urząd Pracy w Oświęcimiu
ul. Wyspiańskiego 10
32-602 Oświęcim
lub
na adres e-mail: zp@pup.oswiecim.pl
Oferty należy złożyć w terminie do 06.12.2017r. do godz. 9.00.

Z podmiotem, którego oferta zostanie wybrana zostanie zawarta umowa. **Wymagany termin realizacji zamówienia od 11.12.2017r. do 21.12.2017r. Umowa zostanie zawarta niezwłocznie po wyborze oferty.**

Do oferty cenowej zawierającej opis (zakres) usług świadczonych w ramach realizacji projektu oraz cenę brutto usług można dołączyć wykaz osób, którzy przeprowadzą audyt wraz ze wskazaniem posiadanych uprawnień i certyfikatów oraz referencje z wykonanych już audytów.

W przypadku przesłania oferty pocztą termin jej wniesienia zostanie zachowany, jeżeli dotrze ona do Zamawiającego przed upływem terminu składana ofert. Oferty, które dotrą do PUP w Oświęcimiu po terminie nie będą rozpatrywane.

W przypadku dodatkowych pytań lub wątpliwości prosimy o kontakt z Panem Dariuszem Stokłosą (33 844-41-44 wew. 1201) lub Ireneuszem Drabikiem (33 844-41-44 wew. 1210).

Powiatowy Urząd Pracy zastrzega sobie prawo:

1. **Zakończenia postępowania bez wyboru żadnej oferty.**
2. **Żądania uzupełniania przez Wykonawców złożonych ofert i załączonych do nich dokumentów, jeśli, Wykonawca nie dostarczy wszystkich żądanych dokumentów czy informacji.**
3. **Żądania wyjaśnienia przez Wykonawcę złożonych ofert i załączonych dokumentów telefonicznie, pocztą elektroniczną lub za pomocą faksu.**

Opis przedmiotu zamówienia

Realizacji kompleksowego projektu z zakresu bezpieczeństwa informacji w Powiatowym Urzędzie Pracy w Oświęcimiu składającego się z następujących elementów:

Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (ISO/IEC 27001)

1. Zakres usługi:

Określenie i sformalizowanie zasad zarządzania w szczególności poprzez wskazanie osób odpowiedzialnych oraz wskazanie podejścia do zapewnienia zasobów niezbędnych do efektywnego zarządzania bezpieczeństwem i zarządzania usługami:

- Weryfikacja i aktualizacja procedury działań korygujących w przypadku niezgodności z wymaganiami systemu zarządzania.
- Aktualizacja Instrukcji zarządzania systemami informatycznymi.
- Weryfikacja i aktualizacja procedury wprowadzania działań zapobiegawczych w przypadku wystąpienia sytuacji mogącej prowadzić do niezgodności z wymaganiami systemu zarządzania.
- Weryfikacja i aktualizacja procedury przeglądu systemu zarządzania, w szczególności określającej częstotliwość przeglądów, zakres i sposób ich przeprowadzania, materiały źródłowe niezbędne do przeprowadzenia przeglądu, tryb wdrażania wniosków.
- Weryfikacja i aktualizacja procedury nadzoru nad dokumentami wchodzącymi w skład systemu zarządzania. W szczególności zostaną określone zasady wersjonowania, zatwierdzania, dystrybucji, przechowywania, archiwizowania i niszczenia dokumentów.
- Weryfikacja i aktualizacja procedury nadzoru nad zapisami, określającej zasady przechowywania, archiwizowania oraz niszczenia zapisów.
- Weryfikacja i aktualizacja dokumentacji dotyczącej zabezpieczeń systemu zarządzania bezpieczeństwem informacji.

Optymalizacja posiadanych przez Zamawiającego dokumentów określających zasady zarządzania bezpieczeństwem informacji, o ile wyniki analizy ryzyka wykażą potrzebę takiej optymalizacji. W opracowaniu mają być wzięte pod uwagę następujące zagadnienia:

- Wymagania w zakresie zabezpieczeń teleinformatycznych.
- Zasady bezpiecznego przetwarzania informacji przez pracowników Zamawiającego.
- Stosowanie zasady czystego biurka i czystego ekranu.
- Zabezpieczenie stacji roboczych.
- Zasady klasyfikacji informacji i postępowania z informacjami klasyfikowanymi.

- Zasady zarządzania dostępem do informacji, w tym nadawania, modyfikacji, odbierania uprawnień oraz przeglądu uprawnień.
- Zasady zarządzania dostępem do usług informatycznych, w tym usług sieciowych.
- Zarządzanie mechanizmami uwierzytelniającymi, w tym hasłami.
- Zasady publikacji informacji.
- Zasady wymiany danych z podmiotami zewnętrznymi.
- Zasady wewnętrznej wymiany danych.
- Zasady postępowania z nośnikami informacji, w tym składowanie i wymiana nośników oraz niszczenie informacji zapisanych na nośnikach.
- Zasady wprowadzania zmian w przetwarzaniu informacji, w szczególności z wykorzystaniem systemów informatycznych, z uwzględnieniem testowania bezpieczeństwa wprowadzanych rozwiązań.
- Wytyczne w zakresie utrzymania dokumentacji zabezpieczeń i systemów informatycznych.
- Weryfikacja przeglądu uprawnień do systemów i zasobów informatycznych pracowników pod względem adekwatności do realizowanych zadań określonych w zakresach obowiązków.
- Zasady zgłaszania podatności w mechanizmach przetwarzających informacje.
- Zasady postępowania w przypadku incydentu naruszenia bezpieczeństwa informacji.
- Zasady kontroli bezpieczeństwa informacji.
- Zasady zarządzania oprogramowaniem.
- Zasady zarządzania kopiami zapasowymi.
- Zasady zarządzania kopiami archiwalnymi.
- Zasady konserwacji i serwisu zabezpieczeń technicznych i systemów informatycznych.
- Zasady monitorowania bezpieczeństwa infrastruktury informatycznej.
- Zasady przygotowania urządzeń IT do ponownego użycia.
- Zasady wycofywania urządzeń IT z użycia.
- Zasady bezpiecznego korzystania z urządzeń mobilnych.
- Zasady bezpiecznej pracy zdalnej.
- Zasady ochrony przed złośliwym oprogramowaniem.
- Zasady zarządzania mechanizmami kryptograficznymi.
- Zasady monitorowania przepisów prawnych związanych z zabezpieczeniem przetwarzanych informacji oraz wprowadzania zmian wynikających z obowiązków prawnych.
- Wytyczne w zakresie ochrony fizycznej i technicznej.
- Wytyczne w zakresie monitorowania przepisów prawnych związanych z ochroną Informacji.
- Wytyczne w zakresie bezpiecznej współpracy z podmiotami zewnętrznymi.
- Wytyczne w zakresie bezpiecznego świadczenia usług związanych z przetwarzaniem informacji.
- Wytyczne w zakresie bezpieczeństwa osobowego w procesach rekrutacji i zarządzania personelem.
- **Dokumenty w zakresie ciągłości działania:**
  a. Strategia ciągłości przetwarzania informacji.
  b. Plan ciągłości działania dla sytuacji uniemożliwienia przetwarzania informacji.
  c. Plan komunikacji kryzysowej na wypadek braku możliwości przetwarzania informacji.
  d. Zasady przeglądu i aktualizacji planu.

e. Weryfikacja obsługi informatycznej pod względem ilości kadr i wystarczających kwalifikacji jakie posiadają pracownicy w celu zachowania obsługi i ciągłość wszystkich systemów obsługiwanych w Urzędzie.

Audyt Legalności Oprogramowania

1. **Zakres audytu:**
   Sprawdzenie spójności, zgodności z przepisami prawa autorskiego oraz stanów licencyjnych:

   - Pełna inwentaryzacja zainstalowanego oprogramowania na stacjach roboczych i serwerach organizacji (około 100 komputerów).
   - Inwentaryzacja dokumentacji licencyjnej (atrybutów legalności) przedstawionej przez organizacje.
   - Weryfikacja zgodności zainstalowanego oprogramowania ze stanem licencyjnym.
   - Wyszukanie i wykazanie plików multimedialnych (audio, video) oraz plików instalacyjnych.

2. **Podsumowanie oraz wnioski z przeprowadzonego audytu:**

   - Sporządzenie raport z audytu, w którym zawarty jest: opis stanu zarządzania oprogramowaniem na dzień audytu, zalecenia naprawcze, zbiorcze zestawienie zainstalowanych aplikacji, zbiorcze zestawienie systemów operacyjnych z wykrytymi kluczami licencyjnymi, zbiorcze zestawienie wykrytych pakietów typu office z kluczami instalacyjnymi, zestawienie plików multimedialnych ze wskazaniem ścieżek dostępu.
   - Nadzór nad zrealizowaniem działań naprawczych.
   - Wystawienie certyfikatu legalności przez firmę.
   - Doradztwo w zakresie zarządzania oprogramowaniem.

Wdrożenie Dokumentacji RODO (Rozporządzenie o Ochronie Danych Osobowych)

1. **Zakres usługi:**
   Audyt wstępny obejmujący:
   - Weryfikację spełnienia wymagań rozporządzenia RODO.
   - Zapoznanie z obowiązującymi procedurami w zakresie ochrony danych osobowych.
   - Rozpoznanie struktury organizacyjnej organizacji.
   - Dokonanie identyfikacji wymagań prawnych oraz biznesowych.

   Projektowanie systemu ochrony danych osobowych poprzez następujące procedury i zagadnienia:
   - Kodeks postępowania
     1. Procedury zarządzania uprawnieniami i upoważnieniami do przetwarzania danych osobowych.
     2. Procedury realizacji i spełnienia obowiązku informacyjnego.
     3. Procedury dotyczące uświadamiania i realizacji szkoleń.

4. Procedury współpracy z podmiotami zewnętrznymi i powierzenia przetwarzania danych osobowych.
5. Procedury zarządzania i realizacji audytów wewnętrznych.
6. Przypisanie odpowiednich ról i odpowiedzialności w zakresie ochrony danych osobowych.

- Polityka ochrony danych osobowych
    1. Procedury dotyczące stosowania kryptografii i pseudonimizacji danych.
    2. Procedury dotyczące ciągłości działania i przywrócenia danych osobowych.
    3. Procedury dotyczące stosowanych środków bezpieczeństwa ochrony organizacyjnej, fizycznej, technicznej.
    4. Procedury zarządzania naruszeniami ochrony danych osobowych.
    5. Procedury dotyczące usuwania danych i utylizacji nośników po utracie ich przydatności.
    6. Procedury dotyczące uwzględniania prywatności w fazie projektowania i profilowania danych osobowych.
- Rejestr czynności przetwarzania
    1. Opis danych kontaktowych do administratora danych i osób funkcyjnych;
    2. Opis celów przetwarzania i kategorii osób, których dane osobowe są przetwarzane.
    3. Opis kategorii odbiorców danych.
    4. Opis planowanych terminów usunięcia danych osobowych.
    5. Ogólny opis stosowanych środków bezpieczeństwa.
- Ocena skutków dla ochrony
    1. Procedury dotyczące identyfikacji rodzajów operacji bądź aktywów przetwarzania danych osobowych.
    2. Procedury oceny niezbędności i proporcjonalności dla analizy ryzyka.
    3. Opis stosowanej metodyki oceny skutków dla ochrony danych osobowych.
    4. Rejestr ryzyk i wyniki szacowania ryzyka.
    5. Opis procedury postępowania z ryzykiem i wyboru środków zaradczych w celu minimalizowania i unikania ryzyka.
    6. Opis postępowania w przypadku konsultacji z organem nadzorczym Urzędem Ochrony Danych Osobowych.
    7. Raportowanie i przekazywanie wyników oceny ryzyka.