Ogłoszenie Nr 7/21

Dyrektor Centrum Usług Informatycznych w Białymstoku
ogłasza nabór na stanowisko:
specjalisty do spraw SZBI w Centrum Usług Informatycznych
w Białymstoku, ul. Warszawska 13 lok.7U

1. Funkcje podstawowe wykonywane na stanowisku:

- Odpowiedzialność za koordynację, planowanie, projektowanie dokumentów, przegląd zarządzania oraz utrzymanie i doskonalenie systemu zarządzania bezpieczeństwem informacji w CUI.
- Zapewnienie zgodności SZBI w CUI z wymaganiami Polskiej Normy PN- ISO/IEC 27001, a w odniesieniu do ustanowionych zabezpieczeń, zarządzania ryzykiem, odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania, zgodności z wymaganiami Polskiej Normy PN- ISO/IEC 27002, PN-ISO/IEC 27005 PN- ISO/IEC 24762.
- Koordynacja działań systemowych w CUI, w tym m.in. audytów zewnętrznych, przeglądów zarządzania, działań korygujących i zapobiegawczych, w zakresie klasyfikacji informacji, analiz ryzyka, przygotowywanie planów postępowania z ryzykiem.
- Prowadzenie audytu wewnętrznego systemu zarządzania bezpieczeństwem informacji w CUI, o którym mowa w § 20 ust. 2 pkt 14 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 2017 r. poz. 2247).
- Przeprowadzanie audytów w zakresie zgodności operacji przetwarzania z prawem, w tym przeprowadzenie inspekcji w podmiotach, z którymi CUI zawiera umowy, w tym umowy powierzenia przetwarzania danych osobowych.
- Nadzorowanie w CUI dokumentacji, zawierającej wymagania dotyczące bezpieczeństwa informacji.
- Szacowanie ryzyka i przeprowadzanie oceny skutków przetwarzania dla ochrony danych w celu identyfikacji ryzyk związanych z bezpieczeństwem informacji przetwarzanych w działalności CUI oraz przygotowanie i uzgadnianie propozycji postępowania w celu optymalnego zabezpieczenia informacji, w tym tworzenie planów zarządzania ryzykiem. Stosowanie metod szacowania ryzyka zgodnych z Polską Normą PN-ISO/IEC 27005.
- Opracowywanie kierunków i planów rozwoju SZBI w CUI, wdrażanie zasad, procedur, instrukcji i regulaminów w obszarze bezpieczeństwa informacji, w tym wsparcie komórek organizacyjnych CUI przy uaktualnianiu procedur w celu określenia zasad bezpiecznego przetwarzania danych z uwzględnieniem wymogów przepisów prawa oraz najlepszych praktyk.
- Zapewnienie integracji SZBI w CUI z procesami realizowanymi przez CUI.
- Opracowywanie rocznych planów audytu SZBI w CUI.

- Aktualizacja dokumentacji SZBI pod kątem merytorycznym, przedkładanie propozycji zmian w dokumentacji kierownikom komórek organizacyjnych CUI oraz Dyrektorowi CUI.
- Dokonywanie klasyfikacji informacji i przeprowadzanie analizy ryzyka w komórkach organizacyjnych CUI.
- Realizacja planu postępowania z ryzykiem w komórkach organizacyjnych CUI.
- Egzekwowanie przestrzegania zasad bezpieczeństwa informacji.
- Szkolenie pracowników w obszarze bezpieczeństwa informacji.
- Udzielanie odpowiedzi na wnioski o udostępnianie informacji publicznej w zakresie działania CUI w obszarze SZBI w celu zapewnienia zgodności z przepisami prawa.

2. Wymagania niezbędne:

- obywatelstwo polskie,
- wykształcenie prawnicze, wyższe informatyczne.
- doświadczenie zawodowe: co najmniej 5 lat stażu pracy w obszarze finansów publicznych,
- co najmniej trzyletnie doświadczenie w samodzielnym realizowaniu zadań z wiązanych z wdrażaniem i rozwijaniem systemów zarządzania bezpieczeństwem informacji,
- odbyte szkolenia w zakresie audytu i kontroli,
- uprawnienia certyfikowanego audytora wiodącego Polskiej Normy PN-ISO/IEC 27001,
- upoważnienie do dostępu do informacji niejawnych o klauzuli „zastrzeżone",
- znajomość języka angielskiego potwierdzona certyfikatem na poziomie B1,
- znajomość ustawy o informatyzacji podmiotów realizujących zadania publiczne,
- znajomość rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych,
- znajomość ustawy o krajowym systemie cyberbezpieczeństwa,
- znajomość rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) zwanego - „RODO",
- znajomość ustawy o ochronie danych osobowych,
- znajomość ustawy o dostępie do informacji publicznej,
- biegła umiejętność obsługi komputera w zakresie MS Office, Excel.
- znajomość wymagań Polskich Norm: PN- ISO/IEC 27001, PN- ISO/IEC 27002, PN-ISO/IEC 27005 PN- ISO/IEC 24762,
- pełna zdolność do czynności prawnych oraz korzystanie z pełni praw publicznych,
- niekaralność za przestępstwo ścigane z oskarżenia publicznego lub umyślne przestępstwo skarbowe.

3. Wymagania dodatkowe:

- co najmniej trzyletnie doświadczenie zawodowe z zakresu samodzielnego prowadzenia audytu i kontroli,
- znajomość języka angielskiego, potwierdzona certyfikatem na poziomie C1,
- umiejętność prowadzenia audytów wewnętrznych w zakresie bezpieczeństwa informacji,
- umiejętność kreatywnego myślenia i rozwiązywania problemów,
- komunikatywność, samodzielność, obowiązkowość, umiejętność pracy w zespole.

4. Wymagane dokumenty:

list motywacyjny; kwestionariusz osobowy lub cv; **oświadczenia**: o posiadaniu obywatelstwa polskiego, oświadczenie o niekaralności za umyślne przestępstwo ścigane z oskarżenia publicznego lub umyślne przestępstwo skarbowe, o pełnej zdolności do czynności