


OFERTY DO	WYMIAR ETATU	STANOWISKA	STATUS	DODATKOWE
13 marca 2018	1	1	archiwalny	

Dyrektor Generalny poszukuje kandydatów\kandydatek na stanowisko:

główny specjalista

do spraw: nadzoru nad bezpieczeństwem teleinformatycznym Ministerstwa Cyfryzacji –
Pełnomocnik Ministra
w Wydziale Bezpieczeństwa Teleinformatycznego, Departament Cyberbezpieczeństwa

MIEJSCE WYKONYWANIA PRACY:

Warszawa

ADRES URZĘDU:

Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa

WARUNKI PRACY

- Nietypowe godziny pracy (w tym dyżury).
- Krajowe lub zagraniczne wyjazdy służbowe.
- Zagrożenie korupcją.
- Częste reprezentowanie urzędu na zewnątrz.
- Praca przy komputerze powyżej 4 godzin.
- Budynek częściowo dostosowany do potrzeb osób poruszających się na wózkach inwalidzkich.

ZAKRES ZADAŃ

- Opracowywanie projektów regulacji wewnętrznych, w tym zarządzeń i wytycznych Ministra Cyfryzacji w zakresie ustanawiania odpowiednich i proporcjonalnych środków ochrony systemów teleinformatycznych Ministerstwa Cyfryzacji.
- Określanie zasad obsługi incydentów naruszających bezpieczeństwo teleinformatyczne dotyczących działalności Ministerstwa Cyfryzacji.
- Sprawowanie nadzoru nad wdrażaniem przepisów i wytycznych Ministra Cyfryzacji odnośnie bezpieczeństwa teleinformatycznego.
- Koordynowanie procesów szacowania ryzyka w Ministerstwie Cyfryzacji w zakresie zagrożeń o charakterze teleinformatycznym. Współpraca z komórką odpowiedzialną za audyt wewnętrzny w zakresie bezpieczeństwa teleinformatycznego.
- Opracowywanie wytycznych dla właścicieli zasobów w zakresie tworzenia dokumentacji bezpieczeństwa, w tym polityk szczegółowych, procedur bezpiecznej eksploatacji, instrukcji stanowiskowych.
- Przygotowywanie wkładów do projektów odpowiedzi na pisma kierowane do Ministra w zakresie swoich kompetencji.
- Współpraca ze służbami i instytucjami w zakresie bezpieczeństwa i ochrony informacji w Ministerstwie Cyfryzacji.
- Uczestniczenie w planowaniu architektury bezpieczeństwa systemów informatycznych realizowanych przez ministerstwo oraz akceptowanie niezbędnych zmian w architekturze bezpieczeństwa, mechanizmów

bezpieczeństwa poszczególnych systemów.

WYMAGANIA NIEZBĘDNE

- Wykształcenie: wyższe magisterskie
- doświadczenie zawodowe: 3 lata na samodzielnym stanowisku w zakresie zarządzania bezpieczeństwem informacji
- Przeszkolenie ze znajomości norm ISO/IEC serii 27000
- Poświadczenie bezpieczeństwa do klauzuli „tajne” w tym NATO i UE lub zgoda na poddanie się procedurze sprawdzającej
- Znajomość języka angielskiego na poziomie B1
- Znajomość „Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 - 2022”
- Znajomość Strategii bezpieczeństwa cybernetycznego UE
- Znajomość aktów prawnych, dokumentów strategicznych dot. problematyki bezpieczeństwa sieci i informacji w Polsce i UE
- Znajomość ustaw: o ochronie danych osobowych, o ochronie informacji niejawnych, Prawo telekomunikacyjne, o informatyzacji działalności podmiotów realizujących zadania publiczne wraz z aktami wykonawczymi
- Znajomość Polskich Norm związanych z bezpieczeństwem informacji
- Umiejętność organizacji pracy własnej
- Zorientowanie na osiąganie celów
- Umiejętność współpracy.
- Skuteczna komunikacja.
- Umiejętność analitycznego myślenia.
- Posiadanie obywatelstwa polskiego
- Korzystanie z pełni praw publicznych
- Nieskazanie prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe

WYMAGANIA DODATKOWE

- Wykształcenie: wyższe magisterskie o profilu systemy informatyczne lub informatyka, lub teleinformatyka, lub telekomunikacja, lub elektronika
- doświadczenie zawodowe: 1 rok w pracy w administracji publicznej
- Studia podyplomowe z zakresu informatyki lub teleinformatyki, lub telekomunikacji
- Specjalistyczne kursy służb ochrony państwa
- Certyfikat audytora wewnętrznego SZBI lub CISA
- Umiejętność planowania i myślenia strategicznego

DOKUMENTY I OŚWIADCZENIA NIEZBĘDNE

- Życiorys/CV i list motywacyjny
- Kopie dokumentów potwierdzających spełnienie wymagania niezbędnego w zakresie wykształcenia
- Kopie dokumentów potwierdzających spełnienie wymagania niezbędnego w zakresie doświadczenia zawodowego / stażu pracy
- Kopie dokumentów potwierdzających spełnienie wymagania niezbędnego w zakresie przeszkolenia ze znajomości norm ISO/IEC serii 27000
- Kopia poświadczenia bezpieczeństwa uprawniającego do dostępu do informacji niejawnych oznaczonych klauzulą „tajne” w tym NATO i UE lub zgoda na poddanie się procedurze sprawdzającej
- Oświadczenie o posiadaniu obywatelstwa polskiego albo kopia dokumentu potwierdzającego posiadanie polskiego obywatelstwa
- Oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych do celów naboru
- Oświadczenie o korzystaniu z pełni praw publicznych
- Oświadczenie o nieskazaniu prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe

DOKUMENTY I OŚWIADCZENIA DODATKOWE

- kopia dokumentu potwierdzającego niepełnosprawność - w przypadku kandydatek/kandydatów, zamierzających skorzystać z pierwszeństwa w zatrudnieniu w przypadku, gdy znajdą się w gronie najlepszych kandydatek/kandydatów
- Kopie dokumentów potwierdzających spełnienie wymagania dodatkowego w zakresie wykształcenia
- Kopie dokumentów potwierdzających spełnienie wymagania dodatkowego w zakresie doświadczenia zawodowego / stażu pracy
- Kopie dokumentów potwierdzających spełnienie wymagania dodatkowego w zakresie odbycia specjalistycznych kursów służb ochrony państwa
- Kopie certyfikatu audytora wewnętrznego SZBI lub CISA

TERMINY I MIEJSCE SKŁADANIA DOKUMENTÓW

- Dokumenty należy złożyć do: 13 marca 2018 r.
- Decyduje data: stempla pocztowego / osobistego dostarczenia oferty do urzędu
- Miejsce składania dokumentów:
Pod adresem:
Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa

z wyraźnym dopiskiem na kopercie i w liście motywacyjnym:
„Główny specjalista/MC/DC/WBT/10.1”

INNE INFORMACJE:

W miesiącu poprzedzającym datę upublicznienia ogłoszenia wskaźnik zatrudnienia osób niepełnosprawnych w urzędzie, w rozumieniu przepisów o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych, nie wynosi co najmniej 6%.

Do składania dokumentów zachęcamy również osoby niepełnosprawne, które spełniają wymagania zwarte w niniejszym ogłoszeniu.

Oświadczenia muszą być podpisane własnoręcznie. Oferty otrzymane po terminie (decyduje data stempla pocztowego) oraz niekompletne nie będą rozpatrywane. Dokumenty złożone w aplikacji nie będą zwracane. Po zakończeniu naboru oferty osób niezatrudnionych zostaną zniszczone. Kandydatki/kandydaci zakwalifikowani do poszczególnych etapów selekcji zostaną powiadomieni telefonicznie lub drogą elektroniczną o ich terminie. Informacja o wyniku naboru na powyższe stanowisko zostanie opublikowana na stronach internetowych: <http://nabory.kprm.gov.pl>, <http://mc.bip.gov.pl> oraz udostępniona w miejscu powszechnie dostępnym w siedzibie Urzędu.

Dodatkowe informacje można uzyskać pod nr tel.: (22) 245 57 63.

Nasz urząd jest pracodawcą równych szans i wszystkie aplikacje są rozważane z równą uwagą bez względu na płeć, wiek, niepełnosprawność, rasę, narodowość, przekonania polityczne, przynależność związkową, pochodzenie etniczne, wyznanie, orientację seksualną czy też jakąkolwiek inną cechę prawnie chronioną.

LEGENDA



Pierwszeństwo dla osób z niepełnosprawnościami

Ogłoszenie z tym symbolem oznacza, że pierwszeństwo w zatrudnieniu mają osoby z niepełnosprawnościami, które spełniają wszystkie następujące warunki:

- złożyły w terminie ofertę wraz z dokumentem potwierdzającym niepełnosprawność,
- spełniają warunki wymienione w ogłoszeniu,
- po rekrutacji znalazły się w gronie najlepszych kandydatów.