Ministerstwo Zdrowia w Warszawie

00-952 Warszawa ul. Miodowa 15

Ogłoszenie nr 134745 / 07.03.2024

Główny Specjalista

Do spraw: bezpieczeństwa cyberprzestrzeni w Wydziale Bezpieczeństwa Teleinformatycznego w Departamencie Innowacji

Pierwszeństwo dla osób z niepełnosprawnościami

Nabór zdalny

Liczba stanowisk	Wymiar etatu	Status	Miejsce pracy	Ważne do	Wynagrodzenie zasadnicze
1	1	nabór w toku	Warszawa ul. Miodowa 15	18 marca 2024 r.	10514,16 zł brutto

Czym będziesz się zajmować

Osoba na tym stanowisku:

- Identyfikuje zagrożenia w cyberprzestrzeni, obsługuje i zarządza incydentami bezpieczeństwa w celu zapewnienia ciągłości funkcjonowania urzędu
- Obsługuje kwarantannę poczty MZ oraz zajmuje się weryfikacją alertów systemu antywirusowego oraz EDR
- Obsługuje zgłoszenia OTRS ścieżki Bezpieczeństwa
- Współpracuje z Centrum e-Zdrowia w zakresie powołania Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) dla obszaru ochrony zdrowia
- Testuje plany awaryjne (odtworzeniowe) i plany ciągłości działania systemów teleinformatycznych Urzędu w ramach ciągłości działania Ministerstwa we współpracy z Centrum e-Zdrowia
- Monitoruje przestrzeganie obowiązujących polityk i procedur, opracowuje i wdraża procedury reagowania na incydenty bezpieczeństwa
- Przeprowadza analizy ryzyka i opracowuje plan postępowania z ryzykiem w zakresie SZBI

Kogo poszukujemy

Potrzebne ci będą (wymagania niezbędne)

- Wykształcenie: wyższe
- Doświadczenie zawodowe co najmniej 3 lata związane z budową i utrzymaniem systemów teleinformatycznych/ infrastruktury techniczno-systemowej

- Upoważnienie do dostępu do informacji niejawnych o klauzuli „zastrzeżone” lub wyrażenie zgody na poddanie się procedurze uzyskania dostępu
- Znajomość ustawy o krajowym systemie cyberbezpieczeństwa
- Znajomość 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,
- Znajomość technologii, norm i standardów z zakresu ochrony informacji i bezpieczeństwa teleinformatycznego
- Znajomość technik ataków na systemy teleinformatyczne
- Znajomość protokołów komunikacyjnych modelu TCP/IP, znajomość rozwiązań typu: SIEM, DLP, anty-malware, wykrywania włamań, WAF
- Posiadanie obywatelstwa polskiego
- Korzystanie z pełni praw publicznych
- Nieskazanie prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe

Dodatkowym atutem będzie (wymagania dodatkowe)

- Wykształcenie: wyższe z zakresu informatyki, automatyki, bezpieczeństwa IT, elektroniki
- Doświadczenie zawodowe co najmniej 1 rok związane z bezpieczeństwem IT / inżynierią wsteczną / obsługą incydentów bezpieczeństwa IT/ zakresem technologii sieciowych
- Znajomość ustawy o krajowym systemie cyberbezpieczeństwa, wraz z aktami wykonawczymi
- Znajomość ustawy o informatyzacji podmiotów realizujących zadania publiczne, wraz z aktami wykonawczymi
- Znajomość standardów z zakresu cyberbezpieczeństwa

Co oferujemy

- Ruchomy czas pracy
- Indywidualny rozkład czasu pracy
- Częściowe wykonywanie pracy poza siedzibą urzędu (praca zdalna, „home office”)
- Możliwość wyjścia w celu załatwienia ważnej sprawy
- Stołówka pracownicza
- Karty sportowe lub dofinansowanie zajęć sportowo-rekreacyjnych
- Dopłata do biletów na imprezy kulturalne
- Pomieszczenie lub stojaki na rowery na terenie urzędu
- Pokój dla rodzica z dzieckiem
- Dopłaty do żłobka, przedszkola i klubu dziecięcego oraz opieki sprawowanej przez opiekuna dziennego
- Dostosowanie planów urlopów pracowników posiadających dzieci w wieku szkolnym i przedszkolnym do terminów wakacji, ferii i przerw świątecznych
- Dofinansowanie do wypoczynku pracowników
- Dofinansowanie do wypoczynku dzieci pracowników
- Stabilne zatrudnienie na umowę o pracę
- Dodatek za wysługę lat (powyżej 5 lat) od 5 do 20% wynagrodzenia zasadniczego w zależności od udokumentowanego stażu pracy
- Możliwość rozwoju kompetencji i kwalifikacji poprzez ciekawe zadania i projekty
- Możliwość doskonalenia zawodowego
- „Trzynaste” wynagrodzenie
- Nagrody jubileuszowe
- Pakiet socjalny (niskooprocentowane pożyczki, pomoc finansowa w trudnych sytuacjach)
- Możliwość wykupienia na preferencyjnych warunkach pakietu ubezpieczeń
- Projekty: profilaktyka „Kierunek-ZDROWIE” oraz „ZDROWIE dla o(d)pornych”,

- Dofinansowanie do zakupu okularów korekcyjnych.

Dostępność

- Nasz urząd jest pracodawcą równych szans. Aplikacje rozważane są 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.
- Do składania ofert zachęcamy również osoby ze szczególnymi potrzebami.
- Jako osoba z niepełnosprawnością możesz skorzystać z pierwszeństwa w zatrudnieniu – złóż wówczas kopię dokumentu potwierdzającego niepełnosprawność.
  W miesiącu poprzedzającym datę upublicznienia ogłoszenia wskaźnik zatrudnienia osób niepełnosprawnych w urzędzie, w rozumieniu przepisów ustawy o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych, był mniejszy niż 6%.

Warunki pracy

- Departament Innowacji mieści się Warszawie przy ul. Miodowej 15 na II piętrze; winda znajduje się w budynku „B”; budynek jest częściowo dostosowany do potrzeb osób niepełnosprawnych poruszających się na wózkach inwalidzkich; w budynku „B” i „C” jest toaleta przystosowana dla osób niepełnosprawnych.
- Praca biurowa wykonywana w pozycji siedzącej przy komputerze, co najmniej 4 godziny dziennie
- Stanowisko zagrożone korupcją
- Obsługa klientów zewnętrznych
- Praca pod dużą presją czasu

Dodatkowe informacje

- Jeśli zostaniesz zakwalifikowany do kolejnego etapu, powiadomimy Cię o tym mailowo (lub telefonicznie – jeżeli nie podałeś adresu e-mail).
- Oświadczenia podpisz odręcznie i wstaw datę ich sporządzenia.
- Oferty kandydatów, którzy nie zostali zatrudnieni, zniszczymy po 3 miesiącach od zakończenia naboru.
- Nie rozpatrzymy oferty, którą otrzymamy po terminie. Dotyczy to też uzupełniania ofert.
- Nie rozpatrzymy oferty, którą nadałeś po terminie. Dotyczy to też uzupełniania ofert.
- Kompletna aplikacja to taka, która zawiera wszystkie wymagane dokumenty i własnoręcznie podpisane oświadczenia.
- Do dokumentów sporządzonych w języku obcym dołącz kopie ich tłumaczenia na język polski sporządzone przez tłumacza przysięgłego.
- Nie przesyłaj wszystkich dokumentów, które uznasz, że mogą Ci pomóc w naborze. Prześlij tylko te, których wymagamy lub zalecamy.
- Zwróć uwagę na warunki pracy, które wskazaliśmy w ogłoszeniu – rzetelnie oceń, czy odpowiada Ci taka praca.
- Złożone przez Ciebie dokumenty zweryfikujemy pod względem formalnym na podstawie zapisów ogłoszenia dotyczących wymaganych i dodatkowych dokumentów.

Planujemy następujące metody/techniki naboru:

- Etap 1: weryfikacja formalna nadesłanych ofert – do drugiego etapu zaproszeni zostaną kandydaci, którzy spełniają wszystkie wymagania formalne
- Etap 2: test wiedzy online, (fakultatywnie)
- Etap 3: rozmowa kwalifikacyjna, w tym sprawdzenie wiedzy.

Pracę możesz rozpocząć od: 2024-04-01

Twoja aplikacja musi zawierać (dokumenty niezbędne)

- 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
- Oświadczenie kandydatki/kandydata, że w okresie od 22 lipca 1944 r. do 31 lipca 1990 r. nie pracowała/nie pracował, nie pełniła/nie pełnił służby w organach bezpieczeństwa państwa i nie była/nie był współpracownikiem tych organów w rozumieniu przepisów ustawy z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944–1990 oraz treści tych dokumentów (Nie dotyczy kandydatek/kandydatów urodzonych 1 sierpnia 1972 r. lub później)
- Upoważnienie do dostępu do informacji niejawnych o klauzuli „zastrzeżone” lub wyrażenie zgody na poddanie się procedurze uzyskania dostępu
- Dokumentami potwierdzającymi spełnienie wymagania niezbędnego w zakresie doświadczenia zawodowego / stażu pracy są m.in. opis stanowiska pracy, zakres czynności, zaświadczenie o zatrudnieniu
- Oświadczenie o posiadaniu obywatelstwa polskiego
- Oświadczenie o korzystaniu z pełni praw publicznych
- Oświadczenie o nieskazaniu prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe

Dołącz, jeśli posiadasz (dokumenty 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
- Dokumenty potwierdzające przeszkolenie z zakresu cyberbezpieczeństwa

Aplikuj do: 18 marca 2024

Aplikuj elektronicznie przez stronę: **https://kariera.mz.gov.pl/?p=2427**
Lub w formie papierowej **w zamkniętej kopercie** na adres: **Ministerstwo Zdrowia, Biuro Administracyjne, ul. Miodowa 15, 00–952 Warszawa z dopiskiem: „Główny specjalista w Wydziale Bezpieczeństwa Teleinformatycznego w Departamencie Innowacji – poz. 2427"**

Zapraszamy również do kontaktu telefonicznego: **882 365 029**

- Dokumenty należy złożyć do: **18.03.2024**
- Decyduje data: **wpływu oferty do urzędu**
- Aplikując, oświadczasz, że znana Ci jest treść informacji na temat przetwarzania danych osobowych w naborze

Przetwarzanie danych osobowych

Dane osobowe są przetwarzane zgodnie z przepisami 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 (RODO).

- Administrator danych i kontakt do niego: Administratorem danych osobowych kandydatek/kandydatów jest Minister Zdrowia z siedzibą w Warszawie, ul. Miodowa 15.
- Kontakt do inspektora ochrony danych: iod@mz.gov.pl.

- Cel przetwarzania danych:
  przeprowadzenie naboru na stanowisko pracy w służbie cywilnej oraz archiwizacja dokumentów po przeprowadzeniu naboru
- Informacje o odbiorcach danych: członkowie komisji naborowej
- Okres przechowywania danych:
  czas niezbędny do przeprowadzenia naboru na stanowisko pracy w służbie cywilnej (z uwzględnieniem 3 miesięcy, w których dyrektor generalny urzędu ma możliwość wyboru kolejnego wyłonionego kandydata, w przypadku, gdy ponownie zaistnieje konieczność obsadzenia tego samego stanowiska), a następnie przez czas wynikający z przepisów o archiwizacji
- Uprawnienia:
  1. prawo dostępu do swoich danych oraz otrzymania ich kopii;
  2. prawo do sprostowania (poprawiania) swoich danych osobowych;
  3. prawo do ograniczenia przetwarzania danych osobowych;
  4. prawo do usunięcia danych osobowych;
     - żądanie realizacji tych praw należy przesłać w formie pisemnej na adres kontaktowy administratora danych, podany powyżej;
  5. prawo do wniesienia skargi do organu nadzorczego - Prezesa Urzędu Ochrony Danych Osobowych (ul. Stawki 2, 00-193 Warszawa).
- Podstawa prawna przetwarzania danych:
  1. art. 6 ust. 1 lit. b *RODO*;
  2. art. 22^1 *Kodeksu pracy*, ustawa z dnia 21 listopada 2008 r. o *służbie cywilnej* oraz ustawa z dnia 14 lipca 1983 r. o *narodowym zasobie archiwalnym i archiwach* w zw. z art. 6 ust. 1 lit. c *RODO*;
  3. art. 6 ust. 1 lit. a *RODO* oraz art. 9 ust. 2 lit. a *RODO*.
- Informacje o wymogu podania danych:
  Podanie danych osobowych w zakresie wynikającym z art. 22^1 *Kodeksu pracy* oraz ustawy *o służbie cywilnej* (m.in. imię, nazwisko, dane kontaktowe, wykształcenie, przebieg dotychczasowego zatrudnienia, wymagania do zatrudnienia w służbie cywilnej) jest dobrowolne, jednak niezbędne, aby uczestniczyć w procesie naboru na stanowisko pracy w służbie cywilnej.

  Podanie innych danych w zakresie nieokreślonym przepisami prawa, zostanie potraktowane jako zgoda na przetwarzanie danych osobowych. Wyrażenie zgody w tym przypadku jest dobrowolne, a zgodę tak wyrażoną można odwołać w dowolnym czasie.

  Jeżeli podane dane będą obejmowały szczególne kategorie danych, o których mowa w art. 9 ust. 1 *RODO*, konieczna będzie wyraźna zgoda na ich przetwarzanie, która może zostać odwołana w dowolnym czasie.
- Inne informacje: podane dane nie będą podstawą do zautomatyzowanego podejmowania decyzji; nie będą też profilowane