



Ministerstwo Spraw Zagranicznych

Numer ogłoszenia:

BOIN 2/2024

Data ukazania się ogłoszenia: 08.02.2024 r.

Nazwa oferowanego stanowiska:

Ministerstwo Spraw Zagranicznych w Warszawie

Dyrektor Generalny Służby Zagranicznej poszukuje kandydatek/kandydatów na stanowisko specjalisty ds. zarządzania bezpieczeństwem teleinformatycznym w Biurze Ochrony Informacji Niejawnych

Wskaźnik zatrudnienia osób niepełnosprawnych w urzędzie

W miesiącu poprzedzającym datę upublicznienia ogłoszenia wskaźnik zatrudnienia osób niepełnosprawnych w urzędzie, w rozumieniu przepisów o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych **jest niższy niż 6%**.

Wymiar etatu: 1

Liczba stanowisk pracy: 2

Adres urzędu:

Ministerstwo Spraw Zagranicznych

Al. J. Ch. Szucha 23

00-580 Warszawa

Miejsce wykonywania pracy:

Warszawa

Zakres zadań wykonywanych przez pracownika na stanowisku pracy:

1. Pełni funkcję inspektora bezpieczeństwa teleinformatycznego, zapewniając zgodne z przepisami prawa przetwarzanie informacji niejawnych w systemach teleinformatycznych.
2. Kontroluje zgodność funkcjonowania systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych z dokumentacją bezpieczeństwa systemów, prowadzi postępowania wyjaśniające w przypadku stwierdzenia naruszenia procedur bezpiecznej eksploatacji w tych systemach oraz analizuje i monitoruje zgłaszane zdarzenia związane z bezpieczeństwem teleinformatycznym.
3. Przeprowadza audyty systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych w celu sprawdzenia ich bezpiecznego funkcjonowania.
4. Bierze udział w procesie zarządzania ryzykiem w systemach teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych w Ministerstwie Spraw Zagranicznych, jednostkach organizacyjnych podległych lub nadzorowanych przez Ministra Spraw Zagranicznych oraz innych jednostkach organizacyjnych eksploatujących systemy teleinformatyczne, których organizatorem jest Minister Spraw Zagranicznych.

5. Opiniuje i inicjuje zmiany dokumentacji w zakresie bezpieczeństwa systemów TI, przeznaczonych do przetwarzania informacji niejawnych, w celu wykrycia i niedopuszczenia do powstania potencjalnej możliwości technicznych zagrożeń dla bezpieczeństwa informacji, zapewniając jednocześnie zgodność dokumentacji z przepisami prawa, zaleceniami ABW, NATO i UE, normami i dobrymi praktykami.
6. Uczestniczy w projektowaniu oraz inicjuje zmiany w systemach TI przeznaczonych do przetwarzania informacji niejawnych w celu zapewnienia: bezpiecznego funkcjonowania systemu, eliminowania technicznych zagrożeń i podatności oraz skutecznej implementacji rozwiązań technicznych i organizacyjnych. Zapewnienia ich zgodności z obowiązującymi regulacjami prawnymi.
7. Analizuje obszar bezpieczeństwa teleinformatycznego w celu eliminowania nowych zagrożeń oraz projektowania i skutecznej implementacji efektywnych rozwiązań technicznych i organizacyjnych, w ramach funkcjonujących w Ministerstwie systemów.
8. Pełni funkcję oficera bezpieczeństwa (INFOSEC Officer) nadzorując bezpieczeństwo materiałów kryptograficznych w Kancelarii Kryptograficznej MSZ.

Warunki pracy:

Warunki dotyczące charakteru pracy na stanowisku i sposobu wykonywania zadań:

1. Krajowe lub zagraniczne wyjazdy służbowe.
2. Zagrożenie naciskami grup przestępczych.
3. Zagrożenie korupcją.
4. Permanentna obsługa klientów zewnętrznych (spoza administracji, np. obywatele, przedsiębiorstwa) lub przeprowadzanie kontroli w innych urzędach.

Miejsce i otoczenie organizacyjno-techniczne stanowiska pracy:

Praca administracyjno-biurowa przy komputerze z monitorem ekranowym powyżej 4 godzin dziennie, wymagająca obsługi również innych urządzeń biurowych. Długotrwałe skupianie wzroku na tej samej płaszczyźnie. Stanowisko pracy zorganizowane w pomieszczeniu biurowym. Bariery architektoniczne: możliwość ograniczonego poruszania się po budynku – obecność wind, brak podjazdów, drzwi z samozamykaczami.

W związku z wyjazdami służbowymi, otoczenie i warunki pracy mogą być różne.

Wymagania związane ze stanowiskiem pracy:

Niezbędne:

Wykształcenie:

wyższe lub równorzędne.

Doświadczenie zawodowe:

Powyżej 1 roku w obszarze teleinformatyki lub audytu wewnętrznego lub ochrony informacji niejawnych lub na podobnym stanowisku.

Pozostałe wymagania niezbędne:

1. Specjalistyczne szkolenie z zakresu bezpieczeństwa teleinformatycznego prowadzonego przez ABW albo SKW lub zgoda na poddanie się szkoleniu.
2. Szkolenie audytora wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001 lub zgoda na poddanie się szkoleniu.
3. Poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą ŚCIŚLE TAJNE, TRES SECRET UE/EU TOP SECRET, NATO COSMIC TOP SECRET lub zgoda na poddanie się postępowaniu sprawdzającemu.
4. Uprawnienia personelu kancelarii kryptograficznej lub zgoda na odbycie specjalistycznego szkolenia dla kandydatów na kierowników oraz członków personelu kancelarii kryptograficzne.

5. Znajomość ustawy o ochronie informacji niejawnych, norm, zaleceń i wytycznych związanych z ochroną informacji niejawnych, norm, zaleceń i wytycznych związanych z bezpieczeństwem systemów teleinformatycznych, norm ISO związanych z zarządzaniem bezpieczeństwem informacji.
6. Znajomość zagadnień związanych z funkcjonowaniem systemów teleinformatycznych oraz z metodykami realizacji audytów teleinformatycznych. Znajomość metod zarządzania oraz szacowania ryzyka w organizacjach.
7. Znajomość zagadnień związanych z kryptograficzną ochroną informacji. Wiedza w zakresie technicznej analizy systemów teleinformatycznych, w tym – w analizy dzienników zdarzeń. Znajomość technicznych zagadnień dotyczących informatyki śledczej oraz metod i technik projektowania systemów teleinformatycznych. Wiedza w zakresie tworzenia skryptów powłok systemowych.
8. Dyspozycyjność - gotowość do częstych wyjazdów służbowych, pracy poza siedzibą ministerstwa, pracy poza granicami kraju.
9. Umiejętność: współpracy, argumentowania, analitycznego myślenia.
10. Zorientowanie na osiąganie celów, odporność na stres.
11. Posiadanie obywatelstwa polskiego.
12. Korzystanie z pełni praw publicznych.
13. Nieskazanie prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe.

Dodatkowe:

Wykształcenie:

Wyższe o profilu informatyka lub telekomunikacja lub elektronika lub elektrotechnika lub mechatronika lub pokrewne lub Studia podyplomowe o profilu bezpieczeństwo teleinformatyczne lub bezpieczeństwo informacji lub pokrewne.

Doświadczenie zawodowe:

Powyżej 2 lat w obszarze bezpieczeństwa teleinformatycznego.

Pozostałe wymagania dodatkowe:

1. Specjalistyczne szkolenia związane z problematyką bezpieczeństwa informacji, poparte certyfikatami.
2. Specjalistyczne szkolenia związane z problematyką bezpieczeństwa teleinformatycznego, poparte certyfikatami.
3. Znajomość języka angielskiego na poziomie A2.

Dokumenty i oświadczenia:

niezbędne:

1. Kopie dokumentów potwierdzających spełnienie wymagania niezbędnego w zakresie wykształcenia.
2. Kopie dokumentów potwierdzających spełnienie wymagania niezbędnego w zakresie doświadczenia zawodowego.
3. Kopie dokumentów potwierdzających spełnienie wymagania niezbędnego w zakresie przeszkolenia lub zgoda na poddanie się szkoleniu .
4. Kopia poświadczenia bezpieczeństwa uprawniającego do dostępu do informacji niejawnych oznaczonych klauzulą ŚCIŚLE TAJNE, TRES SECRET UE/EU TOP SECRET, NATO COSMIC TOP SECRET lub oświadczenie o wyrażeniu zgody na przeprowadzenie postępowania sprawdzającego zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t. j. Dz. U. z 2019 r., poz. 742 oraz z 2022 r. poz. 655, 1933).
5. CV.
6. Kwestionariusz on-line pod adresem <https://system.erecruiter.pl/FormTemplates/RecruitmentForm.aspx?WebID=763e7151d99647d9bb788a2f941b0e6f> lub kwestionariusz aplikacyjny znajdujący się na stronie MSZ (gov.pl/dyplomacja) w zakładce Praca i Kariera – Nabór do MSZ – Nabory: użyteczne

informacje i pliki do pobrania: <https://www.gov.pl/web/dyplomacja/nabory-uzyteczne-informacje-i-pliki-do-pobrania>

7. Oświadczenie o posiadaniu obywatelstwa polskiego.
8. Oświadczenie o korzystaniu z pełni praw publicznych.
9. Oświadczenie o nieskazaniu prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe.
10. Oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych do celów naboru.
11. Oświadczenie o przebiegu kształcenia w zagranicznych podmiotach systemu szkolnictwa wyższego i nauki.
12. Oświadczenie o niewspółpracowaniu z organami bezpieczeństwa państwa w latach 1944-1990 (nie dotyczy kandydatek/kandydatów urodzonych 1 sierpnia 1972 r. lub później).

dotatkowe:

1. Kopia dokumentu potwierdzającego niepełnosprawność – w przypadku kandydatek/kandydatów, którzy zamierzają skorzystać z pierwszeństwa w zatrudnieniu w przypadku, gdy znajdują się w gronie najlepszych kandydatek/kandydatów.
2. Kopia dokumentów potwierdzających spełnienie wymagania dodatkowego w zakresie wykształcenia.
3. Kopia dokumentów potwierdzających spełnienie wymagania dodatkowego w zakresie doświadczenia zawodowego.
4. Kopie dokumentów potwierdzających spełnienie wymagania dodatkowego w zakresie przeszkolenia.

Termin składania dokumentów:

Decyduje data: 01.03.2024 r.

wpływu oferty do urzędu

Miejsce składania dokumentów:

lub Kwestionariusz aplikacyjny on-line (**preferowany**) na stronie:

<https://system.erecruiter.pl/FormTemplates/RecruitmentForm.aspx?WebID=763e7151d99647d9bb788a2f941b0e6f>

lub

Ministerstwo Spraw Zagranicznych
Biuro Spraw Osobowych
Al. J. Ch. Szucha 23
00-580 Warszawa

z dopiskiem na kopercie oraz w aplikacji: **BOIN 2/2024**

Inne informacje:

Proponowane wynagrodzenie:

Proponowane wynagrodzenie zasadnicze brutto od ok. 5250 do ok. 8100 PLN oraz dodatek za usługę lat (zgodnie z art. 90 ustawy z dnia 21 czerwca 2021 r. o służbie cywilnej (t.j. Dz. U. z 2022 r. poz. 1691, z 2023 r. poz. 1195).

Dziennik Podawczy:

czynny w godzinach 8.15 – 16.15. Oferty otrzymane po terminie nie będą rozpatrywane.

Oświadczenie lustracyjne lub informacja o złożeniu oświadczenia lustracyjnego

W służbie cywilnej nie może być zatrudniona osoba, która w okresie od dnia 22 lipca 1944 r. do dnia 31 lipca 1990 r. pracowała lub pełniła służbę w organach bezpieczeństwa państwa lub była 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.

Osoba wybrana do zatrudnienia, która urodziła się przed **1 sierpnia 1972 r.**, będzie zobowiązana do złożenia oświadczenia lustracyjnego lub informacji o złożeniu oświadczenia lustracyjnego (według wzoru określonego w nw. ustawie), zgodnie z art. 7 ustawy z dnia 18 października 2006 roku o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944 – 1990 oraz treści tych dokumentów (Dz. U. z 2020 r. poz. 2141 – j.t. z późn. zm.).

Informacje dotyczące kopii dokumentów potwierdzających spełnianie wymagań

Szczegółowe informacje dotyczące kopii dokumentów potwierdzających spełnianie wymagań niezbędnych oraz dodatkowych znajdują się na stronie Biuletynu Informacji Publicznej MSZ w zakładce Praca i kariera – Praca w MSZ – Zasady i użyteczne informacje:
<https://www.gov.pl/web/dyplomacja/nabory-uzyteczne-informacje-i-pliki-do-pobrania>

Dokumenty w języku polskim opatrzone podpisem

Wszelkie dokumenty załączane do oferty wystawione w języku obcym winny być przetłumaczone na język polski.

Dokumenty winny być opatrzone datą i podpisane własnoręcznie, a następnie odwzorowane cyfrowo w przypadku skorzystania z kwestionariusza aplikacyjnego on-line. Dokumenty złożone w aplikacji nie będą zwracane. Po zakończeniu naboru oferty osób nie wskazanych do zatrudnienia będą zniszczone.

Wymogi dotyczące uznania dyplomu studiów wyższych na uczelni zagranicznej

W przypadku ukończenia studiów wyższych na uczelni zagranicznej, prosimy o przesłanie kopii potwierdzenia uznania dyplomu przez Narodową Agencję Wymiany Akademickiej lub nostryfikacji dyplomu oraz tłumaczenie przysięgłe. Informacje dotyczące uznawalności zamieszczone są na stronie NAWA: <https://nawa.gov.pl/uznawalnosc/wydawanie-informacji-o-zagranicznych-dyplomach>

Kontakt:

W ofercie należy podać adres e-mail oraz numer telefonu. Kandydatki/kandydaci zakwalifikowani będą informowani e-mailem lub telefonicznie o terminie kolejnego etapu naboru.

Kontakt: Wydział Zarządzania Kompetencjami, tel. +48 (22) 523 8751 email: rekrutacja@msz.gov.pl

Informacja o pracodawcy:

Ministerstwo Spraw Zagranicznych 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, orientacje seksualną czy też jakąkolwiek inną cechę prawnie chronioną.

Dane osobowe - klauzula informacyjna

Informacja dotycząca przetwarzania przez MSZ danych osobowych kandydatów biorących udział w procesie rekrutacji na stanowiska w służbie cywilnej, stanowiąca realizację obowiązku określonego w art. 13 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) (Dz. Urz. UE L 119 z 4.05.2016 r., s. 1 oraz Dz. Urz. UE L 127 z 23.05.2018 r., s. 2).

1. Administratorem, w rozumieniu art. 4 pkt 7 RODO, danych osobowych osób biorących udział w naborze jest Minister Spraw Zagranicznych z siedzibą w Polsce, w Warszawie, Al. J. Ch. Szucha 23, 00-580 Warszawa.
2. Minister Spraw Zagranicznych powołał Inspektora Ochrony Danych (IOD), który realizuje swoje obowiązki w odniesieniu do danych przetwarzanych w Ministerstwie Spraw Zagranicznych i placówkach zagranicznych, Al. J. Ch. Szucha 23, 00-580 Warszawa, adres e-mail: iod@msz.gov.pl.
3. Dane osobowe są przetwarzane w celu przeprowadzenia postępowania rekrutacyjnego na wybrane stanowisko w służbie cywilnej:
 - 1) w oparciu o art. 6 ust. 1 lit. c RODO w zakresie wskazanym w art. 22¹ § 1 pkt. 1 – 3 Kodeksu Pracy,
 - 2) w oparciu o art. 6 ust. 1 lit. b RODO w zakresie wskazanym w art. 22¹ § 1 pkt. 4 – 6 Kodeksu Pracy,
 - 3) w oparciu o art. 6 ust. 1 lit. c oraz art. 10 RODO w zakresie danych niezbędnych do weryfikacji kryteriów wskazanych w art. 4 ustawy o służbie cywilnej,
 - 4) w oparciu o art. 9 ust. 2 lit. b RODO w zakresie wskazanym w art. 28 ust. 2b ustawy z dnia 21 listopada 2008 r. o służbie cywilnej,
 - 5) w oparciu o art. 6 ust. 1 lit. a oraz art. 9 ust. 2 lit. a RODO, tj. na podstawie zgody w zakresie danych nie objętych przepisami prawa, które kandydat przekazał z własnej inicjatywy.
4. Podanie danych osobowych wskazanych w przepisach prawa jest niezbędne, aby uczestniczyć w postępowaniu rekrutacyjnym. Konsekwencją ich niepodania będzie brak możliwości udziału w naborze na stanowisko, którego dotyczy ogłoszenie. Podanie innych danych osobowych wykraczających poza zakres wskazany w przepisach prawa zostanie potraktowane jako zgoda na ich przetwarzanie. Wyrażenie zgody jest dobrowolne, zaś zgodę można odwołać w dowolnym czasie, poprzez przesłanie stosownej informacji na adres e-mail: rekrutacja@msz.gov.pl. W przypadku zgody na przetwarzanie danych osobowych szczególnych kategorii, musi być ona wyrażona w sposób wyraźny. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.
5. Dane osobowe zawarte w protokole naboru obejmujące do pięciu najlepszych kandydatów będą przetwarzane przez okres niezbędny do realizacji celu przetwarzania, a następnie przechowywane w celach archiwalnych przez okres 5 lat, zgodnie z przepisami ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2020 r. poz. 164) oraz przepisami wewnętrznymi MSZ wynikającymi z przepisów ww. ustawy. Dane pozostałych kandydatów oraz dane zamieszczone w przesłanych dokumentach zostaną usunięte bezpośrednio po zakończeniu naboru lub po 3 miesiącach od jego zakończenia.
6. Dane osobowe mogą być udostępniane osobom i podmiotom trzecim uprawnionym do dostępu do nich na podstawie obowiązujących przepisów prawa. Dotyczy to w szczególności imion i nazwisk kandydatów, którzy spełniają wymagania formalne w zakresie określonym w ogłoszeniu o naborze oraz wyniku naboru, stanowiącym informację publiczną. Odrębną kategorię odbiorców mogą stanowić podmioty przetwarzające dane osobowe na zlecenie Administratora, w szczególności dostawcy usług IT.
7. Uprawnienia przysługujące osobom, których dane dotyczą:
 - prawo do dostępu do treści swoich danych;
 - prawo do żądania sprostowania danych osobowych, które są nieprawidłowe;
 - prawo do cofnięcia zgody na przetwarzanie danych osobowych, jeżeli była ona podstawą przetwarzania;
 - prawo do usunięcia danych, w szczególności, jeżeli przetwarzanie danych opiera się na zgodzie, w myśl art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO lub dane osobowe są przetwarzane niezgodnie z prawem;

- prawo do ograniczenia przetwarzania danych, w sytuacjach i na zasadach wskazanych w art. 18 RODO.
8. Dane osobowe nie będą przetwarzane w sposób zautomatyzowany, który będzie miał wpływ na podejmowanie decyzji mogących wywołać skutki prawne lub w podobny sposób istotnie na nią wpłynąć, w tym nie będą poddawane profilowaniu.
 9. Osobie, której dane dotyczą przysługuje prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.