Ministerstwo Spraw Wewnętrznych i Administracji w Warszawie

02-591 Warszawa ul. Stefana Batorego 5

Ogłoszenie nr 168371 / 25.09.2026

starszy specjalista/starsza specjalistka

Do spraw: realizacji zadań prawno-regulacyjnych w obszarze bezpieczeństwa infrastruktury teleinformatycznej w Wydziale Bezpieczeństwa Infrastruktury Teleinformatycznej w Departamencie Teleinformatyki

#administracja publiczna #informatyzacja #IT #sprawy wewnętrzne

Pierwszeństwo dla osób z niepełnosprawnościami



Liczba stanowisk	Wymiar etatu	Status	Miejsce pracy	Ważne do	Wynagrodzenie zasadnicze
1	1	nabór w toku	ul. Domaniewska 36/38 02-672 Warszawa	6 października 2026 r.	od 8528,00 zł do 9665,00 zł brutto

Czym będziesz się zajmować

Osoba na tym stanowisku:

- Realizuje obowiązki wynikające z ustawy o krajowym systemie cyberbezpieczeństwa. Opracowuje raporty, analizy oraz sprawozdawczość dotyczącą stanu bezpieczeństwa cyberprzestrzeni infrastruktury resortowej
- Koordynuje i opracowuje dokumentację, w tym procedury i wewnętrzne akty prawne, w zakresie infrastruktury teleinformatycznej oraz cyberprzestrzeni resortu
- Uczestniczy w opracowywaniu i zarządzaniu ciągłością działania w odniesieniu do sieci i systemów teleinformatycznych, w tym dokonuje analiz i szacowania ryzyka dla infrastruktury teleinformatycznej
- Uczestniczy w opracowywaniu i nadzorowaniu polityki zarządzania incydentami i podatnościami
- Współpracuje z instytucjami i podmiotami zewnętrznymi zajmującymi się zwalczaniem cyberprzestępczości, w celu wymiany doświadczeń, analizy zagrożeń i koordynacji działań
- Opiniuje pod kątem bezpieczeństwa informacji dokumentację w procesach zakupowych IT, w tym Opisy Przedmiotu Zamówienia. Rekomenduje adekwatne klauzule bezpieczeństwa oraz weryfikuje umowy z dostawcami pod kątem spełniania standardów ochrony informacji
- Analizuje raporty z audytów, identyfikuje obszary wymagające poprawy oraz opracowuje rekomendacje w celu realizacji zaleceń audytowych. Zapewnia ich wdrażanie oraz uwzględnienie we wszystkich nowych projektach informatycznych realizowanych w Ministerstwie
- Analizuje, opiniuje i opracowuje projekty aktów prawnych pozostających w zakresie bezpieczeństwa teleinformatycznego i cyberprzestrzeni. Zapewnia zgodność wewnętrznych uregulowań z obowiązującymi przepisami prawa, w tym z ustawą o

KSC i dyrektywą NIS2

Kogo poszukujemy

Potrzebne ci będą (wymagania niezbędne)

- Wykształcenie: wyższe w zakresie informatyki lub cyberbezpieczeństwa lub prawa lub administracji
- Co najmniej 1,5 roku doświadczenia zawodowego w obszarze zapewnienia wsparcia prawnego, cyberbezpieczeństwa, bezpieczeństwa teleinformatycznego lub zarządzania bezpieczeństwem informacji
- Powyżej 2 lat doświadczenia zawodowego w obszarze zarządzania ryzykiem, ochrony danych osobowych, kontroli wewnętrznej lub nadzoru nad systemami teleinformatycznymi
- Przeszkolenie przez ABW dla administratorów i inspektorów bezpieczeństwa teleinformatycznego lub zgoda na jego odbycie
- Znajomość przepisów w zakresie cyberbezpieczeństwa, ochrony danych osobowych, bezpieczeństwa teleinformatycznego, infrastruktury krytycznej
- Wiedza z zakresu systemu zarządzania bezpieczeństwem informacji w administracji publicznej
- Znajomość zasad tworzenia aktów prawnych w zakresie bezpieczeństwa teleinformatycznego
- Znajomość zasad i dobrych praktyk stosowanych w systemach bezpieczeństwa teleinformatycznego
- Umiejętność myślenia analitycznego, radzenia sobie w sytuacjach kryzysowych, kreatywność
- Umiejętność organizacji pracy i orientacja na osiąganie celów, umiejętność współpracy, skutecznego komunikowania się, rzetelność, gotowość do doskonalenia zawodowego
- Posiadanie poświadczenia bezpieczeństwa uprawniającego do dostępu do informacji niejawnych oznaczonych klauzulą „ tajne”, " NATO/EU Secret " (na etapie składania dokumentów istnieje możliwość złożenia oświadczenia o wyrażeniu zgody na przeprowadzenie postępowania sprawdzającego dotyczącego dostępu do informacji niejawnych)
- 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 będzie musiała złożyć oświadczenie lustracyjne, jeśli urodziła się przed 1 sierpnia 1972 r.
- Posiadanie obywatelstwa polskiego
- Korzystanie z pełni praw publicznych
- Nieskazanie prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe

Dodatkowym atutem będzie (wymagania dodatkowe)

- Wykształcenie podyplomowe w zakresie cyberbezpieczeństwa lub zarządzania bezpieczeństwem informacji lub zarządzania ryzykiem lub prawa
- Co najmniej 1 rok doświadczenia zawodowego w obszarze audytu bezpieczeństwa, szacowania ryzyka teleinformatycznego
- Przeszkolenie specjalistyczne w zakresie ochrony informacji niejawnych w systemach teleinformatycznych.
- Przeszkolenie specjalistyczne w zakresie ochrony danych osobowych
- Posiadanie certyfikatu określonego w załączniku do rozporządzenia Rady Ministrów z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa lub w załączniku do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 10.09.2010 w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych (Dz.U. nr 177, poz. 1195)

Co oferujemy

- Możliwość rozwoju zawodowego, uczestniczenia w szkoleniach oraz częściowej refundacji kosztów nauki języka obcego, studiów podyplomowych.

- Możliwość rozpoczynania i kończenia pracy w przedziale czasowym zamiast stałych godzin pracy: rozpoczęcie pracy między 7.00 a 9.00 i zakończenie jej po 8h.
- Dodatek za wysługę lat (powyżej 5 lat) od 5 do 20% wynagrodzenia w zależności od udokumentowanego stażu pracy.
- „Trzynaste” wynagrodzenie.
- Dodatek służby cywilnej.
- Nagrody jubileuszowe.
- Odprawy emerytalne i rentowe.
- Dofinansowanie do wypoczynku pracowników i ich dzieci.
- Dofinansowanie do działalności rekreacyjno-sportowej (karta Multisport) organizowanej przez Ministerstwo.
- Możliwość skorzystania z niskooprocentowanej pożyczki mieszkaniowej lub remontowej.
- Możliwość korzystania z Międzyzakładowej Kasy Zapomogowo-Pożyczkowej przy MSWiA.
- Dofinansowanie do szczepień ochronnych przeciw grypie.
- Dofinansowanie do zakupu okularów korekcyjnych/soczewek kontaktowych.
- Możliwość korzystania, po preferencyjnych cenach, z pobytów leczniczych w Sanatoriach Uzdrowiskowych MSWiA w ramach dostępnych miejsc.
- Stojaki / miejsce na rowery w lokalizacji przy ul. Batorego 5, Domaniewskiej 36/38 oraz Al. Szucha 2/4.
- Miejsce parkingowe w lokalizacji przy ul. Batorego 5 oraz Al. Szucha 2/4
- Bufet w lokalizacji ul. Batorego 5.

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.
- 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%.
- Do składania ofert zachęcamy również osoby ze szczególnymi potrzebami.
- Jako osoba ze szczególnymi potrzebami możesz je zgłosić na etapie składania dokumentów.
- Podczas rekrutacji podejmujemy działania, by materiały wykorzystywane w trakcie naboru dostosować do potrzeb osób ze szczególnymi potrzebami (np. udostępnimy materiały wydrukowane większą czcionką).

Warunki pracy

Budynek w Warszawie przy ul. Domaniewskiej 36/38.

Dostęp do budynku, szerokość ciągów komunikacyjnych i drzwi wewnętrznych dostosowane są do potrzeb osób poruszających się na wózkach inwalidzkich. Wewnątrz budynku znajdują się windy ułatwiające poruszanie się, jak również łazienki dostosowane do potrzeb osób poruszających się na wózkach inwalidzkich.

Dodatkowe informacje

- UWAGA! Wzory oświadczeń dostępne są pod adresem https://www.gov.pl/web/mswia/pracuj-z-nami
- Do dokumentów sporządzonych w języku obcym dołącz kopie ich tłumaczenia na język polski.
- W przypadku ukończenia studiów wyższych na uczelni zagranicznej, prześlij kopię potwierdzenia uznania dyplomu przez Narodową Agencję Wymiany Akademickiej lub nostryfikacji dyplomu.
- Weryfikacja spełniania przez kandydatów wymagań formalnych dokonana zostanie na podstawie dokumentów wymienionych w części „TWOJA APLIKACJA MUSI ZAWIERAĆ (DOKUMENTY NIEZBĘDNE)".
- Kompletne aplikacje to takie, które zawierają wszystkie wymagane dokumenty i zostały złożone w terminie wskazanym w ogłoszeniu o naborze. Oferty niekompletne mogą zostać odrzucone.
- Aplikacje składane w wersji papierowej muszą zawierać własnoręcznie podpisane oświadczenia opatrzone datą.
- Kandydaci mogą być poproszeni o udostępnienie do wglądu oryginałów dokumentów, na podstawie których potwierdzane jest spełnianie przez nich warunków określonych w ogłoszeniu.
- Przekazanie dokumentów wymienionych w części „DOŁACZ, JEŚLI POSIADASZ DOKUMENTY" nie jest obowiązkowe, jednak będą one podstawą przeprowadzenia oceny spełniania wymagań dodatkowych przez kandydatów.
- Prosimy o zapoznanie się z informacją dotyczącą przetwarzania danych osobowych zamieszczoną na stronie: https://www.gov.pl/web/mswia/pracuj-z-nami
- Kandydaci zakwalifikowani do poszczególnych etapów selekcji zostaną powiadomieni o ich terminie telefonicznie lub pocztą elektroniczną. Możliwa jest rekrutacja zdalna.
- Informacja o wyniku naboru na powyższe stanowisko zostanie opublikowana na stronach internetowych:
- https://nabory.kprm.gov.pl/wyniki-naborow, https://www.gov.pl/web/mswia/wyniki-naborow-na-wolne-stanowiska-pracy-w-korpusie
- oraz udostępniona w miejscu powszechnie dostępnym w siedzibie Urzędu.
- „Informuje się, że w Ministerstwie Spraw Wewnętrznych i Administracji obowiązuje zarządzenie Nr 32 Dyrektora Generalnego MSWiA z dnia 16 września 2024 r. w sprawie Wewnętrznej procedury dokonywania zgłoszeń naruszeń prawa i podejmowania działań następczych w Ministerstwie Spraw Wewnętrznych i Administracji." [link do zakładki internetowej: Sygnalista – zgłoszenie naruszenia prawa_Zgłoszenie wewnętrzne]

Planujemy następujące metody/techniki naboru:

- weryfikacja ofert pod względem formalnym,
- sprawdzian wiedzy,
- sprawdzian znajomości języka angielskiego,
- rozmowa kwalifikacyjna.

Twoja aplikacja musi zawierać (dokumenty niezbędne)

- SKANY/ZDJĘCIA OŚWIADCZEŃ WYSŁANE MAILOWO NIE SĄ POPRAWNE FORMALNIE. OŚWIADCZENIA WYSŁANE MAILOWO MUSZĄ BYĆ OPATRZONE PODPISEM ELEKTRONICZNYM
- List motywacyjny oraz Curriculum Vitae (CV) – zawierające dane kontaktowe i informacje wynikające z wymagań określonych w ogłoszeniu o naborze
- Oświadczenie o posiadaniu wykształcenia wyższego w zakresie informatyki lub cyberbezpieczeństwa lub prawa lub administracji – zgodnie z wymaganiami niezbędnymi (zawierające informacje z dyplomu ukończenia studiów/ świadectwa ukończenia szkoły tj. nr dokumentu, rodzaj wykształcenia, uczelnia/szkoła, która wydała dyplom/świadectwo, wydział, kierunek, specjalizacja)
- Kopie dokumentów potwierdzających spełnienie wymagania niezbędnego w zakresie doświadczenia zawodowego (co najmniej 1,5 roku doświadczenia zawodowego w obszarze zapewnienia wsparcia prawnego, cyberbezpieczeństwa, bezpieczeństwa teleinformatycznego lub zarządzania bezpieczeństwem informacji), tj. świadectwa pracy lub zaświadczenia lub referencje lub zakresy obowiązków lub opisy stanowisk pracy lub inne dokumenty; należy dołączyć dokumenty potwierdzające rodzaj i długość wymaganego doświadczenia
- Kopie dokumentów potwierdzających spełnienie wymagania niezbędnego w zakresie doświadczenia zawodowego

(powyżej 2 lat doświadczenia zawodowego w obszarze zarządzania ryzykiem, ochrony danych osobowych, kontroli wewnętrznej lub nadzoru nad systemami teleinformatycznymi), tj. świadectwa pracy lub zaświadczenia lub referencje lub zakresy obowiązków lub opisy stanowisk pracy lub inne dokumenty; należy dołączyć dokumenty potwierdzające rodzaj i długość wymaganego doświadczenia

- Kopie dokumentów potwierdzających przeszkolenie przez ABW dla administratorów i inspektorów bezpieczeństwa teleinformatycznego lub zgoda na jego odbycie
- Poświadczenie bezpieczeństwa w zakresie dostępu do informacji niejawnych oznaczonych klauzulą "tajne", "UE/NATO SECRET" (na etapie składania dokumentów istnieje możliwość złożenia oświadczenia o wyrażeniu zgody na przeprowadzenie postępowania sprawdzającego dotyczącego dostępu do informacji niejawnych)
- Oświadczenie, że w okresie od dnia 22 lipca 1944 r. do dnia 31 lipca 1990 r. kandydatka/kandydat nie pracowała/ł, nie pełniła/ł służby w organach bezpieczeństwa państwa i nie była/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
- 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
- Oświadczenie o posiadaniu studiów podyplomowych w zakresie cyberbezpieczeństwa lub zarządzania bezpieczeństwem informacji lub zarządzania ryzykiem lub prawa - zgodnie z wymaganiami dodatkowymi (zawierające informacje z dyplomu ukończenia studiów/ świadectwa ukończenia szkoły tj. nr dokumentu, rodzaj wykształcenia, uczelnia/szkoła, która wydała dyplom/świadectwo, wydział, kierunek, specjalizacja)
- Kopie dokumentów potwierdzających co najmniej 1 rok doświadczenia zawodowego w obszarze audytu bezpieczeństwa, szacowania ryzyka teleinformatycznego, tj. świadectwa pracy lub zaświadczenia lub referencje lub zakresy obowiązków lub opisy stanowisk pracy lub inne dokumenty; należy dołączyć dokumenty potwierdzające rodzaj i długość wymaganego doświadczenia
- Kopie dokumentów potwierdzających przeszkolenie specjalistyczne w zakresie ochrony informacji niejawnych w systemach teleinformatycznych
- Kopie dokumentów potwierdzających przeszkolenie specjalistyczne w zakresie ochrony danych osobowych
- Kopie certyfikatu określonego w załączniku do rozporządzenia Rady Ministrów z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa lub w załączniku do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 10.09.2010 w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych

Aplikuj do: 6 października 2026

W formie papierowej na adres: **Ministerstwo Spraw Wewnętrznych i Administracji**
BKSiO
ul. Stefana Batorego 5
02-591 Warszawa
Z dopiskiem na kopercie DT-WBIT-10 starsz-y/a specjalist-a/ka

OSOBIŚCIE: w godz. 8.00-16.00
Biuro Przepustek
ul. Rakowiecka 2a
Warszawa

ELEKTRONICZNIE:
• ePUAP: /MSWIA/domyslna oraz /MSWIA/SkrytkaESP
• e-Doręczenia: AE:PL-56316-74543-JDVGW-18
• e-mail: rekrutacja@mswia.gov.pl

OŚWIADCZENIA WYSYŁANE ELEKTRONICZNIE NALEŻY PODPISAĆ:
• PROFILEM ZAUFANYM lub
• CERTYFIKATEM KWALIFIKOWANYM lub
• PODPISEM ELEKTRONICZYM E-DOWODU.

WZORY OŚWIADCZEŃ: https://www.gov.pl/web/mswia/pracuj-z-nami

Zapraszamy również do kontaktu telefonicznego: **(47) 728 13 82 lub (47) 728 32 84**
lub mailowego na adres: **rekrutacja@mswia.gov.pl**

Więcej o pracy na stronie urzędu: **https://www.gov.pl/web/mswia/pracuj-z-nami**

- Dokumenty należy złożyć do: **06.10.2026**
- 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 - KLAUZULA INFORMACYJNA

Administratorem danych osobowych osób aplikujących o pracę w MSWiA jest Minister Spraw Wewnętrznych i Administracji, mający siedzibę w Warszawie przy ul. Stefana Batorego 5, kod pocztowy: 02-591.

Kontakt: tel. (22) 2500 112 lub fax (22) 601 39 88 lub pisemnie na adres siedziby.

Administrator wyznaczył inspektora ochrony danych, z którym, za pośrednictwem poczty elektronicznej iod@mswia.gov.pl, może się Pani/Pan skontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z ich przetwarzaniem. Dane osoby aplikującej do służby cywilnej w odpowiedzi na ogłoszenie o naborze w MSWiA przetwarzane są w celu realizacji rekrutacji na stanowisko w służbie cywilnej, na podstawie przepisów ustawy o służbie cywilnej, Kodeksu pracy oraz przepisów dotyczących bezpieczeństwa.

Dane osobowe przetwarzane są zgodnie z rozporządzeniem 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) – zwane dalej RODO.

Odbiorcami danych będą podmioty uprawnione na mocy przepisów prawa oraz podmioty działające na zlecenie administratora.

Podanie danych wymaganych przepisami prawa jest niezbędne do przeprowadzenia procesu rekrutacji. Niepodanie tych danych spowoduje brak Pani/Pana udziału w procesie rekrutacji.

Podanie danych w zakresie wykraczającym poza katalog danych określonych w przepisach prawnych jest dobrowolne i nie stanowi wymogu przeprowadzenia procesu rekrutacji (m. in. wizerunku, numeru PESEL). W tym zakresie osobie przesyłającej aplikację w odpowiedzi na ogłoszenia o naborze przysługuje prawo do dostępu do treści tych danych, ich sprostowania oraz żądania ograniczenia ich przetwarzania, a także do ich usunięcia.

W przypadku przetwarzania danych podanych dobrowolnie przysługuje Pani/Panu również prawo do cofnięcia zgody w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

Aplikacje będą niszczone po upływie okresu niezbędnego do przeprowadzenia naboru na stanowisko pracy w służbie cywilnej, uwzględniając art. 33 ustawy o służbie cywilnej, jednakże nie później niż po upływie terminu wynikającego z przepisu art. 291 Kodeksu pracy.

Osobie przesyłającej aplikację w odpowiedzi na ogłoszenia o naborze przysługuje prawo dostępu do treści danych oraz ich sprostowania oraz żądania ograniczenia ich przetwarzania w przypadkach określonych w RODO.

Przysługuje Pani/Panu również prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych, tj. Prezesa Urzędu Ochrony Danych Osobowych mającego siedzibę w Warszawie przy ul. Moniuszki 1A, kod pocztowy:

00-014.