

Ministerstwo Infrastruktury w Warszawie

00-928 Warszawa Chałubińskiego 4/6

Ogłoszenie nr 158829 / 19.12.2025

Zastępca Dyrektora

Do spraw: kierowania Sektorowym Zespołem Reagowania na Incydynty Bezpieczeństwa Komputerowego CSIRT INFRASTRUKTURA, Biuro Zarządzania Kryzysowego

#administracja publiczna #informatyzacja

Pierwszeństwo dla osób z niepełnosprawnościami

Nabór zdalny



Liczba stanowisk

Wymiar etatu

Status

Miejsce pracy

Ważne do

1

1

nabór w toku

Warszawa
Chałubińskiego 4/6

11 stycznia
2026 r.

Czym będziesz się zajmować

Osoba na tym stanowisku:

- Kieruje realizacją zadań oraz sprawuje nadzór nad działalnością Sektorowego Zespołu Reagowania na Incydynty Bezpieczeństwa Komputerowego CSIRT INFRASTRUKTURA.
- Podejmuje decyzje dotyczące wydatkowania środków w zakresie zadań Sektorowego Zespołu Reagowania na Incydynty Bezpieczeństwa Komputerowego CSIRT INFRASTRUKTURA, w tym wnioskuje o udzielenie zamówienia publicznego, zawiera umowy w imieniu właściwego Członka Kierownictwa Ministerstwa / Dyrektora Generalnego oraz sprawdza pod względem merytorycznym dokumenty potwierdzające poniesienie wydatku. Opracowuje materiały do projektu budżetu państwa oraz sprawozdania z wykonania budżetu państwa w zakresie działania Sektorowego Zespołu Reagowania na Incydynty Bezpieczeństwa Komputerowego CSIRT INFRASTRUKTURA. Bierze udział w przygotowywaniu projektów planów inwestycyjnych w zakresie budowy, rozwoju i utrzymania systemów teleinformatycznych.
- Koordynuje i prowadzi nadzór nad sprawami w zakresie realizacji działań niezbędnych do osiągnięcia gotowości operacyjnej CSIRT INFRASTRUKTURA, poprzez wsparcie projektu utworzenia sektorowego zespołu cyberbezpieczeństwa dla sektorów, dla których organem właściwym do spraw cyberbezpieczeństwa jest Minister, zgodnie z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, w szczególności zapewnienia kompletności i aktualności dokumentacji CSIRT INFRASTRUKTURA, realizacji działań informacyjnych dotyczących CSIRT INFRASTRUKTURA, jego struktury, modelu pracy i podstawowych usług, realizacji działań szkoleniowych dla nadzorowanych podmiotów w zakresie procedur zgłaszania incydentów i współpracy z CSIRT INFRASTRUKTURA.
- Kieruje oraz pełni nadzór nad działaniami przygotowującymi do realizacji przez CSIRT sektorowe zadań wskazanych w art. 44 ustawy o krajowym systemie cyberbezpieczeństwa, a w szczególności do przyjmowania zgłoszeń o incydentach poważnych oraz wsparcie w obsłudze tych incydentów w sektorach transport oraz zaopatrzenie w wodę pitną i jej dystrybucja.
- Koordynuje i prowadzi nadzór nad sprawami w zakresie zapewnienia dostępu do informacji przetwarzanych w systemach

teleinformatycznych wykorzystywanych przez Zespół oraz zapewnienia bezpieczeństwa tych systemów i informacji w nich przetwarzanych.

- Koordynuje i prowadzi nadzór nad sprawami w zakresie realizacji zobowiązań wynikających z ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne oraz z Krajowych Ram Interoperacyjności, w zakresie wykorzystywanych rozwiązań teleinformatycznych, będących we właściwości Zespołu
- Koordynuje i prowadzi nadzór nad współpracą z Wydziałem Zarządzania Systemami Teleinformatycznymi w zakresie realizacji zadań związanych z zapewnieniem dostępu do informacji przetwarzanych w utrzymywanych systemach teleinformatycznych.

Kogo poszukujemy

Potrzebne ci będą (wymagania niezbędne)

- Wykształcenie: wyższe magisterskie lub równorzędne
- Doświadczenie zawodowe co najmniej 3 lata w zarządzaniu zespołem ds. cyberbezpieczeństwa lub co najmniej 5 lat w obszarze cyberbezpieczeństwa w tym doświadczenie w zarządzaniu incydentami cyberbezpieczeństwa
- Znajomość języka angielskiego na poziomie B2 lub w zakresie umożliwiającym co najmniej swobodne korzystanie z dokumentacji technicznej, prowadzenie komunikacji służbowej w formie pisemnej, telefonicznej oraz bezpośredniej
- Znajomość przepisów ustawy o krajowym systemie cyberbezpieczeństwa oraz dyrektywy NIS 2
- Znajomość norm, standardów i dobrych praktyk branżowych (co najmniej dwóch spośród: PN-EN ISO/IEC 27001, NIST, MITRE ATT&CK, OWASP)
- Znajomość zasad i praktyk zarządzania ryzykiem, w tym ryzykiem łańcucha dostaw oraz ryzykiem systemowym
- Znajomość przepisów ustawy o finansach publicznych
- Umiejętność zarządzania personelem
- Umiejętność podejmowania decyzji i odpowiedzialność
- Umiejętność organizacji pracy i zorientowanie na osiągnięcie celów
- Skuteczna komunikacja
- Posiadanie poświadczenia bezpieczeństwa do klauzuli TAJNE, NATO Secret i UE Secret lub gotowość do poddania się procedurze weryfikacyjnej upoważniającej do dostępu do informacji niejawnych, zgodnie z przepisami ustawy o ochronie 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: wyższe na kierunku informatyka lub telekomunikacja lub automatyka lub cyberbezpieczeństwo lub zarządzanie kryzysowe lub bezpieczeństwo narodowe/wewnętrzne
- Doświadczenie zawodowe w zespołach operacyjnych typu CSIRT/CERT lub SOC; doświadczenie w pracy z operatorami usług kluczowych lub podmiotami infrastruktury krytycznej; doświadczenie w projektach związanych z zarządzaniem bezpieczeństwem informacji, zapewnieniem ciągłości działania, szacowaniem ryzyka, przeprowadzaniem testów penetracyjnych lub audytami bezpieczeństwa.
- Znajomość przepisów RODO, rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności oraz ustawy o zarządzaniu kryzysowym
- Posiadanie certyfikatów: CISM lub CISSP lub audytora wiodącego systemu zarządzania bezpieczeństwem informacji (ISO 27001) lub audytora wewnętrznego systemu zarządzania ciągłością działania (ISO 22301).

Co oferujemy

- ciekawą pracę
- udział w kluczowych dla kraju projektach w organizacji z tradycjami
- elastyczne godziny pracy, bardzo przyjazną lokalizację (dogodny dojazd środkami komunikacji miejskiej, pociągami, kolejką WKD, SKM)
- możliwość częściowej pracy zdalnej
- dodatkowe wynagrodzenie tzw. „trzynastka”, dodatek za wysługę lat
- bogaty pakiet szkoleń, refundację nauki języka obcego i studiów podyplomowych
- atrakcyjny pakiet socjalny w formie systemu kafeteryjnego oferujący nie tylko dofinansowanie wypoczynku i kart sportowych, pożyczki pracownicze na preferencyjnych warunkach, ale też ciekawe rabaty na bilety do kina i inne rozrywki
- refundację okularów korekcyjnych
- możliwość wykupienia w preferencyjnej cenie pakietu medycznego, polisy na życie i zniżkowej legitymacji PKP
- wsparcie psychologiczne pracowników
- udogodnienia dla rowerzystów - stojaki na rowery na terenie ministerstwa, prysznic
- preferencyjne ceny posiłków w kantine znajdującej się na terenie ministerstwa

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 ze szczególnymi potrzebami możesz je zgłosić na etapie składania dokumentów.
- Umożliwiamy osobom ze szczególnymi potrzebami korzystanie z własnych urządzeń i rozwiązań wspomagających pracę (np. pomoc asystenta lub trenera pracy).
- Zwiększamy czas poszczególnych metod i technik naboru dla osób 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

Ministerstwo zajmuje trzy budynki „A”, „B” i „C” o następujących uwarunkowaniach technicznych:

- węzeł sanitarny przystosowany do potrzeb osób z niepełnosprawnością w budynku „B” (parter) oraz w budynku „A” (dostęp przy pomocy osób trzecich)
- wejście do budynków przystosowane do potrzeb osób z niepełnosprawnością
- szerokość drzwi i ciągi komunikacyjne w budynkach przystosowane do potrzeb osób z niepełnosprawnością
- windy dostosowane do potrzeb osób z niepełnosprawnością
- brak podjazdu dla osób z niepełnosprawnością na wysoki parter w budynku A, na którym usytuowana jest jedna z sal konferencyjnych

Inne warunki, dotyczące charakteru stanowiska pracy:

- praca przy komputerze oraz/lub przy użyciu urządzeń biurowych: fax, ksero, skaner
- zagrożenie korupcją

Dodatkowe informacje

- Jeśli zostaniesz zakwalifikowany do kolejnego etapu, powiadomimy Cię o tym mailowo (lub telefonicznie – jeżeli nie podałeś adresu e-mail).
- Jeśli ofertę składasz elektronicznie, własnoręcznie podpisane oświadczenia dołącz w formie zeskanowanych dokumentów. Przed rozmową kwalifikacyjną poprosimy Cię o dostarczenie oryginałów tych oświadczeń (do wglądu).
- Oświadczenia podpisz odręcznie i wstaw datę ich sporządzenia.
- 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 przysyłaj 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.

Informacja o metodach naboru:

- weryfikacja formalna nadesłanych ofert
- możliwość przeprowadzenia testu wiedzy merytorycznej
- rozmowa kwalifikacyjna (możliwość przeprowadzenia rozmowy przez MS Teams)
- badanie kompetencji kierowniczych (testy psychologiczne lub case study)

Nie rozpatrujemy ofert, które zostały dostarczone po terminie.

UWAGA Jeśli planujesz wysłać aplikację w formie papierowej, zadбай o to, aby wpłynęła do nas w wyznaczonym terminie. Liczy się data wpływu do urzędu.

W przypadku aplikacji elektronicznej - załączniki znajdujące się w udostępnionej w internecie przestrzeni dyskowej (tzw. chmury) nie będą pobierane.

Ministerstwo zastrzega sobie prawo do kontaktu tylko z kandydatami, których oferty spełniają wymagania formalne.

Wzór wymaganych oświadczeń jest dostępny na stronie internetowej:

- <https://www.gov.pl/web/infrastruktura/nabor-w-sluzbie-cywilnej-z-wylaczeniem-stanowisk-wyzszych>

UWAGA Oświadczenia należy podpisać, podając datę aktualną na dzień złożenia dokumentów.

W Ministerstwie Infrastruktury możesz zgłosić naruszenie prawa w trybie określonym w Wewnętrznej procedurze dokonywania zgłoszeń naruszeń prawa i podejmowania działań następczych w Ministerstwie Infrastruktury, stanowiącej Załącznik do Zarządzenia nr 15 Dyrektora Generalnego z dnia 25 września 2024 r. w sprawie ustalenia wewnętrznej procedury zgłaszania informacji o naruszeniach prawa i podejmowania działań następczych.

Szczegóły znajdują się na naszej stronie pod adresem:

<https://www.gov.pl/web/infrastruktura/wewnetrzne-zgloszenia-naruszenia-prawa>

Twoja aplikacja musi zawierać (dokumenty niezbędne)

- CV
- Kopie dokumentów potwierdzających spełnienie wymagania niezbędnego w zakresie wykształcenia
- Oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych (nadmiarowych, nie związanych z wymaganiami i

dokumentami określonymi w ogłoszeniu) przekazanych do celów naboru

- Kopie dokumentów potwierdzających spełnienie wymagania niezbędnego w zakresie doświadczenia zawodowego - np. kopie świadectw pracy, zaświadczeń o zatrudnieniu, opisów stanowisk, zakresów czynności lub kopie innych zaświadczeń (należy potwierdzić zamknięty okres i obszar tematyczny doświadczenia zawodowego)
- Kopie dokumentów potwierdzających posiadanie poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych o klauzuli TAJNE, NATO Secret i UE Secret lub zgoda na poddanie się procedurze sprawdzającej
- 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. Dotyczy kandydatek/kandydatów urodzonych przed 1 sierpnia 1972 r.
- 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 znajdują 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 - np. kopie świadectw pracy, zaświadczeń o zatrudnieniu, opisów stanowisk, zakresów czynności lub kopie innych zaświadczeń (należy potwierdzić zamknięty okres i obszar tematyczny doświadczenia zawodowego)
- Kopie certyfikatów: CISM lub CISSP lub audytora wiodącego systemu zarządzania bezpieczeństwem informacji (ISO 27001) lub audytora wewnętrznego systemu zarządzania ciągłością działania (ISO 22301).

Aplikuj do: 11 stycznia 2026

Aplikuj mailowo na adres: **rekrutacja@mi.gov.pl**, w temacie wpisz: **Ogłoszenie nr 158829 / 19.12.2025**.

Lub w formie papierowej **w zamkniętej kopercie** z dopiskiem: **"ogłoszenie nr 158829"** na adres: **Ministerstwo Infrastruktury**

ul. Chałubińskiego 4/6; 00-928 Warszawa

Dokumenty, z dopiskiem na kopercie „Oferta pracy CSIRT-1/25”, należy przesłać lub złożyć w siedzibie MI w Kancelarii Głównej w godzinach 9:30-16:00

lub mailowo: rekrutacja@mi.gov.pl

Zapraszamy również do kontaktu telefonicznego: **22 630 18 24**

lub mailowego na adres: **rekrutacja@mi.gov.pl**

- Dokumenty należy złożyć do: **11.01.2026**
- 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

Zgodnie z art. 13 ust. 1 i 2 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), informuję, że: 1) administratorem Pani/Pana danych osobowych jest Minister Infrastruktury z siedzibą w Warszawie, przy ul. Chałubińskiego 4/6, zwany dalej „Administratorem danych”; 2) Pani/Pana dane osobowe przetwarzane są w celu realizacji naboru kandydatów do korpusu służby cywilnej, zgodnie z ustawą z dnia 21 listopada 2008 r. o służbie cywilnej; 3) podstawą przetwarzania Pani/Pana danych osobowych jest ustawa z dnia 21 listopada 2008 r. o służbie cywilnej, Kodeks pracy oraz udzielona przez Panią/Pana zgoda w zakresie w jakim zostały przez Panią/Pana podane dane dodatkowe (nadmiarowe)

niewymagane przez wskazane akty prawne; 4) administrator danych przewiduje możliwość powierzenia przetwarzania danych innym podmiotom świadczącym na rzecz Administratora danych usługi z zakresu IT; 5) zgodnie z art. 29 ww. ustawy o służbie cywilnej imiona i nazwiska kandydatów, którzy spełniają wymagania formalne, oraz wynik naboru stanowią informację publiczną w zakresie objętym wymaganiami określonymi w ogłoszeniu o naborze; 6) podanie danych osobowych jest dobrowolne, ale niepodanie danych, które są wymagane przepisami ww. ustaw, lub brak zgody na przetwarzanie danych podanych dodatkowo, będzie skutkowało odrzuceniem oferty kandydata; 7) posiada Pani/Pan prawo do: • żądania dostępu do treści swoich danych osobowych, ich sprostowania lub ograniczenia przetwarzania, • wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych, • cofnięcia zgody i usunięcia danych w zakresie danych, które zostały podane dodatkowo (nadmiarowo) i nie są wymagane przez wskazane akty prawne; 8) Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu; 9) Pani/Pana dane osobowe będą przechowywane przez okres 10 lat, zgodnie z regulacjami wewnętrznymi wydanymi na podstawie art. 6 ust. 2 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z2018 r. poz. 217, z późn. zm.) w zakresie: imię i nazwisko oraz miejsce zamieszkania (miasto). Pozostałe dane będą przechowywane przez okres 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) 10) dane kontaktowe do Inspektora ochrony danych w Ministerstwie Infrastruktury: Inspektor ochrony danych, Ministerstwo Infrastruktury, ul. Chałubińskiego 4/6, 00-928 Warszawa, adres e-mail: inspektor.RODO@mi.gov.pl