

<b>WOJSKOWY INSTYTUT TECHNICZNY UZBROJENIA W ZIELONCE</b>	
<b>Stanowisko</b>	specjalista informatyk/specjalistka informatyki
<b>Wymiar etatu</b>	Umowa na okres próbny
<b>Wydział</b>	specjalista informatyk
<b>Wynarodzenie brutto</b>	
<b>Zakres wykonywanych zadań</b>	<p>Administracja siecią i infrastrukturą: Zarządzanie firewallem Fortinet FortiGate, konfiguracja i utrzymanie infrastruktury sieciowej (przełączniki, routery, access pointy), administracja sieciami bezprzewodowymi WiFi, zarządzanie VLAN i routingiem, zarządzanie połączeniami VPN SSL i IPSec, diagnostyka i naprawa awarii sieciowych oraz zdalna obsługa oddziałów terenowych.</p> <p>Cyberbezpieczeństwo i firewall.</p> <p>Definiowanie i wdrażanie polityk bezpieczeństwa: konfiguracja reguł dostępu, geo-blocking i filtrowanie ruchu, monitoring systemu FortiClient EMS, analiza logów w FortiAnalyzer, zarządzanie systemem antywirusowym ESET, reagowanie na incydenty bezpieczeństwa, prewencja ataków DDoS.</p> <p>Administracja serwerami i wirtualizacją: Zarządzanie środowiskiem VMware (instalacja, konfiguracja i migracja maszyn wirtualnych, zarządzanie zasobami CPU/RAM/storage), administracja serwerami plików Windows Server i Synology, zarządzanie strukturą katalogów i uprawnieniami, mapowanie dysków przez GPO, migracja danych, monitoring wydajności i planowanie pojemności.</p> <p>Active Directory i polityki grupowe: tworzenie i zarządzanie kontami użytkowników i grupami, administracja politykami grupowymi (GPO), reset i odblokowanie kont, zarządzanie strukturą organizacyjną w AD.</p> <p>Helpdesk i wsparcie użytkowników: obsługa zgłoszeń użytkowników, zdalna pomoc przez AnyDesk, instalacja i konfiguracja drukarek sieciowych, szkolenia użytkowników, wsparcie techniczne dla oddziałów terenowych.</p> <p>Sprzęt IT i dokumentacja: inwentaryzacja sprzętu, diagnostyka i naprawa podzespołów, obsługa UPS / agregatu, prowadzenie dokumentacji systemów IT, planowanie zakupów sprzętu i oprogramowania, organizacja stanowisk pracy dla nowych pracowników.</p> <p>Szkolenia i rozwój: szkolenie praktykantów, przekazywanie wiedzy użytkownikom końcowym</p>
<b>Warunki pracy</b>	<ol style="list-style-type: none"> <li>1. Miejsce pracy: specjalista informatyk</li> <li>2. Stanowisko pracy: specjalista informatyk/specjalistka informatyki</li> </ol>
<b>Wymagania niezbędne</b>	<ol style="list-style-type: none"> <li>1. Wyższe na kierunku: informatyka, teleinformatyka, elektronika, cyberbezpieczeństwo, lub wyższe oraz technik informatyk</li> <li>2. Co najmniej 2 lata doświadczenia na stanowisku administratora sieci, systemów IT lub pokrewnym</li> <li>3. Język Angielski first certyfikat</li> <li>4. Samodzielność i inicjatywa w rozwiązywaniu problemów technicznych.</li> <li>5. Odporność na stres i umiejętność działania pod presją czasu.</li> <li>6. Dokładność i skrupulatność (dokumentacja, procedury bezpieczeństwa)</li> <li>7. Administracja firewallem: konfiguracja i zarządzanie firewallem klasy enterprise</li> <li>8. (Fortinet FortiGate lub równoważny).</li> <li>9. Zarządzanie siecią: Konfiguracja VLAN, routingu, przełączników i połączeń</li> <li>10. VPN.</li> <li>11. Administracja Windows Server i AD: Zarządzanie serwerami plików, Active</li> </ol>

	<ol style="list-style-type: none"> <li>12. Directory, GPO i uprawnieniami.</li> <li>13. Wirtualizacja: Administracja środowiskiem VMware, Hyper-V lub Proxmox.</li> <li>14. Systemy bezpieczeństwa: obsługa systemów antywirusowych (ESET lub</li> <li>15. równoważny).</li> <li>16. Diagnostyka i wsparcie użytkowników: Helpdesk, zdalna pomoc, diagnozowanie</li> <li>17. problemów sprzętowych i programowych</li> </ol>
<p><b>Wymaganie dodatkowe</b></p>	<ol style="list-style-type: none"> <li>1. Studia podyplomowe z zakresu sieci komputerowych, cyberbezpieczeństwa,</li> <li>2. administracji IT lub zarządzania infrastrukturą.</li> <li>3. Mile widziane wykształcenie wyższe techniczne kierunkowe: Informatyka,</li> <li>4. teleinformatyka, elektronika, cyberbezpieczeństwo.</li> <li>5. Co najmniej 5 lat doświadczenia na stanowisku administratora sieci lub</li> <li>6. systemów IT lub pokrewnym</li> <li>7. Proaktywność w zakresie bezpieczeństwa, Chęć dzielenia się wiedzą</li> <li>8. (mentoring, szkolenia wewnętrzne), Zdolności organizacyjne i planistyczne.</li> <li>9. Analiza logów bezpieczeństwa: praca z FortiAnalyzer lub innym systemem</li> <li>10. SIEM</li> <li>11. Skryptowanie i automatyzacja: PowerShell, Bash lub inny język skryptowy</li> <li>12. Strona 2 z 2</li> <li>13. Administracja NAS Synology: Zarządzanie serwerem plików Synology w rolach</li> <li>14. serwer plików, serwer kopii zapasowych.</li> </ol>

<p><b>Wymagane dokumenty</b></p>	<ol style="list-style-type: none"> <li>1. list motywacyjny podpisany odręcznie,</li> <li>2. życiorys (CV) z przebiegiem nauki i pracy zawodowej podpisany odręcznie,</li> <li>3. kserokopie świadectw pracy dokumentujące wymagany staż pracy,</li> <li>4. lub/i zaświadczenie o zatrudnieniu w przypadku pozostawania w stosunku pracy poświadczony własnoręcznie za zgodność z oryginałem,</li> <li>5. kwestionariusz osobowy dla osoby ubiegającej się o zatrudnienie (do pobrania ze strony: <a href="http://www.witu.mil.pl">www.witu.mil.pl</a> - strona Główna/ Kariera/ Pliki do pobrania/ Kwestionariusz osobowy),</li> <li>6. kserokopie dokumentów potwierdzających posiadane,</li> <li>7. wykształcenie i kwalifikacje zawodowe,</li> <li>8. inne dokumenty o posiadanych kwalifikacjach i umiejętnościach,</li> <li>9. inne dokumenty, których konieczność przedłożenia wynika z ogłoszenia o rekrutacji, niewymienione wcześniej,</li> <li>10. podpisane odręcznie jedno oświadczenie kandydata zawierające: <ol style="list-style-type: none"> <li>a. oświadczenie o posiadaniu obywatelstwa polskiego,</li> <li>b. wyrażenie zgody na przetwarzanie danych osobowych (do pobrania ze strony <a href="http://www.witu.mil.pl">www</a>),</li> <li>c. oświadczenie o treści:  „Na podstawie art. 6 ust. 1 lit. a 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 tych danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych), wyrażam zgodę na przetwarzanie moich danych osobowych przez Wojskowy Instytut Techniczny Uzbrojenia w Zielonce, w celu wzięcia udziału w rekrutacji na wolne stanowisko w Wojskowym Instytucie Technicznym Uzbrojenia w Zielonce. Zostałem (łam) poinformowany (a) o możliwości wycofania zgody w każdym czasie poprzez przestanie oświadczenia o wycofaniu zgody na adres mailowy: <a href="mailto:kadry@witu.mil.pl">kadry@witu.mil.pl</a>, mam świadomość, że wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie tej zgody.”</li> </ol> </li> </ol>
----------------------------------	--

<b>Termin składania dokumentów</b>	<ol style="list-style-type: none"><li>1. termin składania dokumentów: 2026-05-12,</li><li>2. miejsce składania dokumentów: Wojskowy Instytut Techniczny Uzbrojenia - Kancelaria Jawna lub na adres rekrutacje@witu.mil.pl,</li><li>3. decyduje data wpływu do: WITU.</li></ol>
<b>Informacje dodatkowe</b>	<ol style="list-style-type: none"><li>1. Wymagane dokumenty aplikacyjne należy składać w zamkniętej kopercie z dopiskiem: „Oferta pracy na stanowisko: specjalista informatyk/specjalistka informatyki w specjalista informatyk. Prosimy na kopercie umieścić również swoje imię i nazwisko.</li><li>2. Pracownik Referatu kadr skontaktuje się z każdym kandydatem spełniającym wymagania formalne mailowo w celu potwierdzenia otrzymania dokumentów aplikacyjnych oraz przekazania informacji o następnych etapach rekrutacji.</li><li>3. Aplikacje, które nie spełniają warunków formalnych zostaną komisyjnie zniszczone lub odesłane kandydatom, o ile umieszczą w aplikacji prośbę o ich odesłanie.</li></ol>