

TZ.040.1.2026.TZ1

Słupsk, dnia 22 stycznia 2026 roku

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia „Świadczenie usług informatycznych na potrzeby Zarządu Infrastruktury Miejskiej w Słupsku” jest świadczenie usług informatycznych dla Zarządu Infrastruktury Miejskiej w Słupsku.

Oznaczenia przedmiotu zamówienia we Wspólnym Słowniku Zamówień (CPV):

CPV: 72000000-5 – Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia

2. Przedmiotem zamówienia jest bieżąca obsługa informatyczna oraz nadzór nad posiadanymi przez ZIM w Słupsku urządzeniami i oprogramowaniem we wszystkich siedzibach ZIM, tj. ul. Grotgera 13, ul. Rabina dr. Maxa Josepha 4, ul. Wisławy Szymborskiej 7, ul. Towarowej 10. Do czynności objętych przedmiotem zamówienia należą:
 - 1) administrowanie, konserwacja i nadzór nad prawidłowym funkcjonowaniem sprzętu komputerowego oraz oprogramowania;
 - 2) administrowanie, konserwacja i nadzór nad prawidłowym funkcjonowaniem sieci komputerowej, serwerów, usług informatycznych i baz danych;
 - 3) stała kontrola bezpieczeństwa sieci komputerowej, w tym zabezpieczenie antywirusowe oraz niezwłoczne reagowanie na zagrożenia;
 - 4) instalacja i konfiguracja oprogramowania systemowego i aplikacyjnego na stacjach roboczych;
 - 5) konfiguracja i instalacja zakupionego sprzętu komputerowego i peryferyjnego na stanowiskach pracy;
 - 6) nadawanie uprawnień dostępowych i nadzór nad prawidłowym funkcjonowaniem systemu uwierzytelniania użytkowników;
 - 7) administrowanie, konserwacja i nadzór nad prawidłowym funkcjonowaniem systemu archiwizacji danych;
 - 8) ewidencjonowanie w sposób elektroniczny sprzętu komputerowego (marka, model, parametry techniczne) i oprogramowania (nazwa oprogramowania przypisana do danego stanowiska) Zleceniodawcy na własne potrzeby w celu szybszej diagnozy występujących problemów; w przypadku żądania ze strony Zamawiającego Wykonawca prześle niniejsze zestawienia uprawnionym przedstawicielom Zamawiającego;
 - 9) wsparcie użytkowników w zakresie obsługi sprzętu komputerowego, urządzeń peryferyjnych i oprogramowania;
 - 10) analiza błędów, nieoczekiwanych lub nietypowych zdarzeń, niezgodnych z założeniami zachowań systemów informatycznych oraz współpraca z dostawcami oprogramowania w celu wyeliminowania wykrytych nieprawidłowości;
 - 11) współpraca z dostawcami oprogramowania w celu dokonania zmian w użytkowanych systemach pod kątem potrzeb zgłaszanych przez Zamawiającego;
 - 12) nadzór nad prawidłową wymianą danych pomiędzy oprogramowaniem Zamawiającego pochodzącym od różnych dostawców;
 - 13) usuwanie awarii w posiadanym przez Zamawiającego oprogramowaniu i sprzęcie oraz współdziałanie gdy do usunięcia awarii lub usterki oprogramowania lub sprzętu, w tym sieciach informatycznych, poszczególnych zestawach komputerowych konieczna jest interwencja producenta bądź podmiotu posiadającego prawa autorskie;
 - 14) doradztwo w przedmiocie umowy, w tym w szczególności z zakresu identyfikacji potrzeb, opracowania i bieżącej aktualizacji strategii informatyzacji Zleceniodawcy, zapewniającej doskonalenie zarządzania jednostką i jej funkcjonowania;
 - 15) bieżąca obsługa i nadzór nad funkcjonowaniem monitoringu CCTV będącego w zasobach zamawiającego (bieżąca konfiguracja oprogramowania w tym instalacja programowa nowych kamer)
 - 16) Możliwości korzystania z konsultacji telefonicznych oraz mailowych; dedykowane wyłącznie dla Zamawiającego adresy email oraz numery telefonów.
 - 17) usuwania awarii sprzętu oraz oprogramowania w przypadku stwierdzenia przez Zamawiającego błędu w jego funkcjonowaniu;
 - 18) instalowania nowych wersji wyszczególnionego oprogramowania zgodnie z wytycznymi Zamawiającego;
 - 19) awaryjnego odtwarzania stanu oprogramowania i zgromadzonych danych archiwizowanych przez Zamawiającego na jego wniosek;
 - 20) konsultacji w sprawach rozbudowy, rekonfiguracji, finansowania infrastruktury objętej niniejszą umową;

- 21) optymalizowania konfiguracji oprogramowania i sprzętu, uwzględniające potrzeby Zamawiającego;
- 22) wsparcie użytkowników końcowych: Rozwiązywanie problemów technicznych związanych z systemami operacyjnymi (Windows, Linux, macOS), oprogramowaniem biurowym (Office 365), urządzeniami peryferyjnymi (drukarki, skanery), sieciami LAN/WAN oraz sprzętem komputerowym;
- 23) administracja systemami: Zarządzanie i administracja serwerami Windows Server, Linux, Active Directory (AD), oraz innymi systemami zarządzania tożsamością i dostępem. Konfiguracja i utrzymanie usług sieciowych, takich jak VPN, VoIP oraz serwery pocztowe;
- 24) zarządzanie infrastrukturą sieciową: Instalacja, konfiguracja i utrzymanie sprzętu sieciowego (np. routery, przełączniki, urządzenia Ubiquiti, Mikrotik, FortiGate), zapewnienie bezpieczeństwa sieci, oraz monitorowanie wydajności sieci;
- 25) diagnozowanie i naprawa sprzętu: Identyfikacja i rozwiązywanie problemów związanych ze sprzętem komputerowym, urządzeniami mobilnymi;
- 26) zarządzanie wirtualizacją: Konfiguracja i utrzymanie maszyn wirtualnych przy użyciu technologii takich jak VMware, Hyper-V, Proxmox, VirtualBox;
- 27) zarządzanie bezpieczeństwem informacji: aktualizacja, implementacja i monitorowanie polityk bezpieczeństwa IT (m. in. Załącznika nr 9 do Polityki Ochrony Danych ZIM czyli Instrukcji Zarządzania Systemami Informatycznymi), zarządzanie uprawnieniami dostępu oraz ochrona przed zagrożeniami cybernetycznymi;
- 28) wsparcie przy projektach IT: Udział w planowaniu, wdrażaniu i zarządzaniu projektami IT, w tym projektami związanymi z automatyzacją procesów (PowerShell, Bash), migracją danych oraz wdrażaniem nowych systemów,
- 29) wyznaczenie ASI (Administratora Systemów Informatycznych),
- 30) przeprowadzanie okresowych szkoleń dla wszystkich pracowników Zamawiającego,
- 31) wypełnianie pozostałych, niewymienionych powyżej obowiązków wskazanych w paragrafie 19 Rozporządzenia z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

3. Wymagania względem wykonawcy w zakresie doświadczenia oraz zasobów technicznych:

- 1) Do realizacji przedmiotu zamówienia Wykonawca wyznaczy minimum pięć osób, które będą odpowiedzialne za różne obszary zarządzania IT. Wykonawca zobowiązuje się zapewnić w siedzibie ZIM przy ul. Grottgera 13 stacjonarny dyżur informatyka w godzinach urzędowania jednostki tj. 8:00-15:00. W razie potrzeby osoba ta zapewnia wsparcie informatyczne w pozostałych siedzibach ZIM (tj. przy ul. Rabina dr. Maxa Josepha 4, ul. Wisławy Szymborskiej 7, ul. Towarowej 10). Zapewni to bezpośrednie wsparcie techniczne oraz możliwość szybkiego reagowania na ewentualne problemy. Każda osoba wyznaczona do realizacji zamówienia musi posiadać minimum 3-letnie doświadczenie w pracy na stanowisku związanym z IT, w tym zarządzanie systemami, sieciami oraz wsparcie użytkowników. Doświadczenie powinno być potwierdzone odpowiednimi dokumentami lub referencjami.
- 2) wykonawca musi wykazać, że w okresie ostatnich 12 miesięcy świadczył nieprzerwanie kompleksowe usługi informatyczne w formie zdalnej oraz stacjonarnej dla minimum trzech różnych podmiotów publicznych. Usługi te powinny obejmować zarządzanie i administrację infrastrukturą IT, wsparcie użytkowników, monitorowanie bezpieczeństwa oraz bieżącą konserwację i optymalizację systemów informatycznych. Łączna wartość świadczonych usług dla tych podmiotów publicznych musi wynosić co najmniej 250 tys. zł. Wykonawca powinien przedstawić stosowne referencje potwierdzające spełnienie tego warunku.
- 3) Wykonawca musi wykazać się minimum 5-letnim doświadczeniem w zarządzaniu systemami Windows Server 2019. Wymagana jest znajomość oraz praktyczne doświadczenie w konfiguracji i zarządzaniu usługami takimi jak Active Directory, DNS, DHCP, DFS, WSUS oraz CA (Certificate Authority). Wykonawca powinien dostarczyć dowody na swoje kompetencje w postaci certyfikatów, referencji lub dokumentacji projektowej, która potwierdza realizację podobnych projektów.
- 4) Wykonawca musi posiadać minimum 5-letnie doświadczenie w zarządzaniu sieciami komputerowymi, z naciskiem na bezpieczeństwo sieciowe. Obejmuje to wiedzę i umiejętności w zakresie konfiguracji VLAN, tworzenia i zarządzania politykami bezpieczeństwa oraz zarządzania firewallami i innymi zabezpieczeniami

sieciowymi. Wykonawca powinien dostarczyć szczegółowy opis zrealizowanych projektów związanych z zarządzaniem sieciami, które potwierdzą jego kompetencje w tym zakresie.

- 5) W celu realizacji przedmiotu zamówienia Wykonawca musi posiadać w dniu złożenia oferty wdrożone oprogramowanie do zdalnego dostępu, zarządzania oraz wsparcia technicznego, które umożliwia bezpieczne i szyfrowane połączenia z urządzeniami klientów w czasie rzeczywistym. Oprogramowanie to powinno oferować kompleksową funkcjonalność, obejmującą możliwość zdalnego sterowania urządzeniami, przesyłania plików, zdalnego monitorowania i diagnozowania problemów, a także wsparcie dla szerokiej gamy systemów operacyjnych i urządzeń. Oprogramowanie powinno być przystosowane do obsługi dużej liczby użytkowników i sesji w środowisku korporacyjnym, z możliwością centralnego zarządzania dostęпами oraz generowania szczegółowych raportów z przeprowadzonych operacji. Wdrożone rozwiązanie powinno być w pełni zintegrowane z istniejącą infrastrukturą IT dostawcy, zapewniając szybkie i efektywne wsparcie techniczne, zgodne z najwyższymi standardami bezpieczeństwa i ochrony danych.
- 6) Wykonawca powinien posiadać wdrożone i wykorzystywane w swojej firmie oprogramowanie do zarządzania projektami, zadaniami oraz zgłoszeniami, które umożliwia planowanie, monitorowanie postępu prac oraz zarządzanie incydentami. System powinien oferować funkcje śledzenia zadań, zarządzania przepływem pracy, generowania raportów oraz współpracy zespołowej. Ponadto, oprogramowanie powinno mieć możliwość dostosowania do procesów firmy, zapewniając pełną przejrzystość i kontrolę nad realizowanymi projektami.
- 7) Wykonawca powinien posiadać wdrożone i aktywnie wykorzystywane w swojej firmie rozwiązanie do zarządzania centralą telefoniczną, umożliwiające prowadzenie rozmów telefonicznych przez internet (VoIP), integrację z systemami CRM oraz obsługę wideokonferencji i czatów. Rozwiązanie to powinno być zainstalowane i użytkowane w pełnym zakresie funkcjonalności, zarówno w środowisku lokalnym, jak i chmurowym.
- 8) Wykonawca zapewni gotowość serwisową helpdesk pod dedykowanym numerem telefonu oraz adresem e-mail w trybie 24h/7/365 dni w tym monitoring infrastruktury zamawiającego. Wykonawca wskaże dedykowaną osobę koordynującą realizowane prace przez zespół Wykonawcy.
- 9) Wykonawca w dniu złożenia oferty powinien posiadać ważną polisę ubezpieczeniową, która obejmuje następujące elementy: Ubezpieczenie odpowiedzialności cywilnej konsultantów IT z limitem minimum 800 000 PLN na jedno i wszystkie roszczenia lub serie roszczeń. Ubezpieczenie odpowiedzialności cywilnej i administracyjnej za naruszenie RODO oraz szkód cyber minimum 500 000 PLN na jedno i wszystkie roszczenia lub serie roszczeń. Naruszenie obowiązku zachowania tajemnicy Zamawiającego minimum 500 000 PLN na jedno i wszystkie roszczenia lub serie roszczeń. Oszczerstwo, zniesławienie lub pomówienie Zamawiającego minimum 1 000 000 PLN na jedno i wszystkie roszczenia lub serie roszczeń. Naruszenie praw własności intelektualnej Zamawiającego minimum 100 000 PLN na jedno i wszystkie roszczenia lub serie roszczeń. Wykonawca jest zobowiązany do posiadania polisy ubezpieczeniowej w dniu składania oferty oraz przez cały okres trwania umowy. Polisa powinna pokrywać wszystkie wskazane ryzyka i odpowiadać wymaganym limitom oraz sublimitom odpowiedzialności. W dniu składania oferty, Wykonawca musi przedstawić aktualne zaświadczenie lub certyfikat ubezpieczenia, potwierdzający spełnienie powyższych warunków. Ponadto, Wykonawca zobowiązuje się do regularnego odnawiania polisy oraz dostarczania potwierdzeń jej ważności na żądanie zamawiającego przez cały okres trwania umowy.
- 10) Wykonawca powinien w dniu złożenia oferty posiadać kod NCAGE w zakresie obsługi jednostek centralnych, przetwarzania danych, obsługi urządzeń wejścia/wyjścia, pamięci komputerowych, sprzętu wspierającego przetwarzanie danych (np. zasilacze UPS), materiałów eksploatacyjnych używanych w systemach IT, takich jak dyski, taśmy oraz pozostałych komponentów używanych w systemach informatycznych. Wykonawca powinien być zweryfikowany przez Wojskowe Centrum Normalizacji Jakości i Kodyfikacji i uznany za wiarygodnego partnera, który posiada odpowiednie zasoby, kompetencje i infrastrukturę do realizacji usług wsparcia informatycznego na wymaganym poziomie. Jest to wymóg minimalizujący ryzyko związane z wyborem niewłaściwego wykonawcy.
- 11) Wykonawca musi zapewnić, że jego infrastruktura kolokacyjna jest zlokalizowana w co najmniej dwóch różnych centrach danych zarządzanych przez niezależnych operatorów. Centra te muszą być fizycznie oddzielone, aby zminimalizować ryzyko związane z awariami lokalnymi lub katastrofami. Operatorzy zarządzający infrastrukturą muszą być całkowicie niezależni od siebie pod względem własności, zarządzania i operacji, aby uniknąć sytuacji, w której awaria jednego operatora wpływa na infrastrukturę zarządzaną przez drugiego.
- 12) Wykonawca musi zapewnić całodobowy monitoring strony internetowej, obejmujący zarówno jej bezpieczeństwo jak i wydajność. Usługa powinna obejmować regularne aktualizacje strony, motywu oraz zainstalowanych wtyczek, zabezpieczenie za pomocą firewalla, regularne kopie zapasowe w chmurze (co

najmniej dwa razy dziennie), optymalizację strony, skanowanie w poszukiwaniu luk w zabezpieczeniach oraz monitorowanie wydajności i SEO. Usługa musi zawierać zabezpieczenie przed nieautoryzowanymi próbami dostępu (firewall), blokowanie prób włamań, szyfrowanie danych, oraz regularne skanowanie w celu wykrywania luk w zabezpieczeniach. Kopie zapasowe powinny być przechowywane w chmurze (np. AWS) i umożliwiać szybkie odzyskanie strony. Wykonawca musi przedstawić dokumentację dotyczącą stosowanych środków bezpieczeństwa oraz procedur ochrony danych. Wykonawca musi przedstawić dokumentację potwierdzającą doświadczenie w świadczeniu podobnych usług dla innych klientów. Należy przedstawić co najmniej trzy referencje od klientów, u których Wykonawca realizował podobne projekty w ostatnich pięciu latach.

- 13) Wykonawca musi dostarczać miesięczne raporty zawierające szczegółowe informacje o wykonanych pracach, w tym dane z Google Analytics, oraz raporty dotyczące wydajności strony (Google PageSpeed i Yslow) oraz SEO. Raporty powinny być dostarczane w formie czytelnej i zrozumiałej dla klienta.
- 14) Wykonawca musi dostarczać miesięczne raporty zgłoszeń zawierające szczegółowe informacje o zrealizowanych usługach i przeprowadzonych pracach w minionym miesiącu rozliczeniowym. Raport powinien zawierać dane takie jak: liczba zarejestrowanych zgłoszeń, status zarejestrowanych zgłoszeń oraz ich kategorie i podkategorie, forma udzielonej pomocy, osoba przydzielona do realizacji.
- 15) Wykonawca powinien stosować formalne procedury zarządzania zmianami i konfiguracją, które obejmują planowanie, dokumentowanie, zatwierdzanie i weryfikowanie zmian w systemach informatycznych. Należy przedstawić dokumentację potwierdzającą stosowanie takich procedur oraz dowody na ich skuteczność.
- 16) Wykonawca jest zobowiązany do prowadzenia i aktualizowania Bazy Wiedzy, która będzie zawierała procedury operacyjne, awaryjne, dokumentację techniczną, szczegółowe opisy systemów, konfiguracji i obsługi infrastruktury IT. Dokumentacja powinna być na bieżąco aktualizowana, aby odzwierciedlała wszelkie zmiany w konfiguracji systemów oraz wprowadzane modyfikacje.
- 17) Wykonawca jest zobowiązany do stosowania najlepszych praktyk zarządzania usługami IT zgodnych z wytycznymi ITIL (Information Technology Infrastructure Library). W szczególności, Wykonawca powinien zaimplementować i stosować procesy ITIL w obszarach takich jak zarządzanie incydentami, zarządzanie problemami, zarządzanie zmianami, zarządzanie konfiguracją oraz zarządzanie dostępem. Procesy te powinny być zgodne z aktualnymi wersjami ITIL i dostosowane do specyficznych potrzeb zamawiającego.