



## Opis przedmiotu zamówienia

### A. Wprowadzenie

Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja oprogramowania wspierającego elastyczne formy organizacji pracy, mającego na celu umożliwienie pracownikom zdalnego dostępu do zasobów firmy, zapewniając jednocześnie wysoki poziom bezpieczeństwa oraz integrację z istniejącymi systemami informatycznymi. W ramach zamówienia przewiduje się również wdrożenie systemu zarządzania tożsamością i dostępem, co pozwoli na centralne zarządzanie uprawnieniami użytkowników.

### B. Przedmiot zamówienia:

#### 1. Dostawa oprogramowania – licencje:

- 1.1. 3 szt. Windows Server 2025 Standard - 2 Core (dla 1 serwera zarządzania tożsamością oraz 2 serwerów terminalowych)
- 1.2. 130 szt. Windows Server 2025 - 1 User CAL
- 1.3. 40 szt. Windows Server 2025 Remote Desktop Services - 1 User CAL

**2. Instalacja i konfiguracja oprogramowania na serwerach:** Wykonawca zobowiązany jest do zainstalowania i skonfigurowania oprogramowania na serwerach, zgodnie z wymaganiami Zamawiającego.

**3. Integracja z istniejącymi systemami:** Oprogramowanie musi zostać zintegrowane z obecnie działającymi systemami informatycznymi, aby zapewnić spójność i ciągłość działania infrastruktury IT. Oprogramowanie Infomedica i AMMS.

**4. Przeprowadzenie testów funkcjonalnych i bezpieczeństwa:** Wykonawca zobowiązany jest do przeprowadzenia testów funkcjonalnych i bezpieczeństwa, które potwierdzą poprawność działania oprogramowania oraz jego zgodność z wymaganiami Zamawiającego.

**5. Szkolenie administratorów systemu:** W ramach wdrożenia przewiduje się przeprowadzenie szkoleń dla administratorów systemu Zamawiającego w postaci 8 godzin szkoleniowych.



**6. Wdrożenie systemu zarządzania tożsamością i dostępem**, który umożliwi centralne zarządzanie poświadczeniami i uprawnieniami użytkowników. Wdrożenie i konfiguracja oprogramowania, w tym instalacji na serwerach oraz integracja z istniejącymi systemami informatycznymi, co zapewni spójność i ciągłość działania infrastruktury IT.

#### **6.1. Zakres usług wdrożenia Active Directory**

6.1.1. Przeprowadzenie analizy środowiska Klienta.

6.1.2. Dobór odpowiednich licencji i ilości Windows Server oraz licencji CAL dla użytkowników, po wykonaniu analizy środowiska.

6.1.3. Przygotowanie projektu usługi katalogowej Active Directory.

6.1.3.1. Projekt struktury logicznej katalogu

6.1.3.1.1. Las

6.1.3.1.2. Domeny

6.1.3.1.3. Jednostki organizacyjne w ramach domeny

- Komputery
- Użytkownicy
- Grupy
- Drukarki
- Inne jednostki organizacyjne

6.1.3.1.4. Konwencja nazewnictwa obiektów katalogu

- Stacje robocze
- Serwery
- Konta użytkowników
- Obiekty zasad grup

6.1.3.1.5. Obiekty GPO (Group Policy Object)

- Zasady wykorzystania
- Zastosowanie GPO
- Zarządzanie GPO

6.1.3.2. Projekt struktury fizycznej katalogu

6.1.3.2.1. Lokacje usługi katalogowej

6.1.3.2.2. Podsieci oraz łącza pomiędzy lokacjami

6.1.3.2.3. Rozmieszczenie i konfiguracja kontrolerów domeny

6.1.3.2.4. Topologia replikacji danych katalogu

6.1.3.3. Usługi wspierające Active Directory



- 6.1.3.3.1. Usługi rozwiązywania nazw DNS
  - 6.1.3.3.2. Usługi synchronizacji czasu
  - 6.1.3.3.3. Usługi dodatkowe
  - 6.1.3.4. Model zabezpieczeń i delegacji uprawnień
    - 6.1.3.4.1. Grupy bezpieczeństwa
    - 6.1.3.4.2. Obiekty
    - 6.1.3.4.3. Zasady polityk grupowych
    - 6.1.3.4.4. Dostęp
    - 6.1.3.4.5. Uprawnienia administracyjne
    - 6.1.3.4.6. Uprawnienia operatorskie
    - 6.1.3.4.7. Model bezpieczeństwa Active Directory
  - 6.1.4. Konfiguracja usługi katalogowej Active Directory.
    - 6.1.4.1. Utworzenie domeny, instalacja roli kontrolerów domeny oraz serwera DNS
    - 6.1.4.2. Konfiguracja lasu, domen oraz serwera DNS.
    - 6.1.4.3. Utworzenie schematu organizacyjnego Active Directory.
    - 6.1.4.4. Utworzenie jednostek organizacyjnych, lokacji oraz obiektów GPO.
    - 6.1.4.5. Utworzenie użytkowników i grup użytkowników.
    - 6.1.4.6. Konfiguracja polityk bezpieczeństwa.
    - 6.1.4.7. Konfiguracja polityk grupowych.
    - 6.1.4.8. Instalacja drukarek na serwerze oraz konfiguracja serwera wydruku.
  - 6.1.5. Testy działania środowiska Active Directory.
- 6.2. Zakres usług wdrożenia VPN**
- 6.2.1. Przygotowanie koncepcji dostępów z poziomu połączenia zdalnego
  - 6.2.2. Synchronizacja danych dostępowych z AD w celu wykorzystania do połączeń zdalnych
  - 6.2.3. Konfiguracja i uruchomienie połączeń zdalnych
  - 6.2.4. Konfiguracja dostępów sieciowych
  - 6.2.5. Testy poprawności działania połączenia zdalnego
  - 6.2.6. Przygotowanie instrukcji dla użytkowników
  - 6.2.7. Przygotowanie dokumentacji powdrożeniowej
  - 6.2.8. Wsparcie przy pierwszych połączeniach

**6.3. Przygotowanie dokumentacji technicznej, obejmującej:**



6.3.1. Opis funkcjonalności systemu: Dokumentacja powinna zawierać szczegółowy opis funkcjonalności systemu, co pozwoli na pełne zrozumienie jego możliwości i sposobu działania.

6.3.2. Procedury zarządzania tożsamościami i dostępem: Dokumentacja powinna zawierać procedury zarządzania tożsamościami i dostępem użytkowników, co pozwoli na efektywne zarządzanie uprawnieniami dostępu do zasobów firmy.

## **C. Wymagania dodatkowe.**

**1. Wymagania funkcjonalne.** Oprogramowanie powinno spełniać następujące wymagania funkcjonalne:

- 1.1. Bezpieczne połączenie z zasobami firmy: Oprogramowanie musi zapewniać bezpieczne połączenie, które chroni dane przesyłane między użytkownikami a infrastrukturą organizacji.
- 1.2. Obsługa aplikacji poprzez serwery terminalowe: Użytkownicy powinni mieć możliwość uruchamiania aplikacji zdalnie, co pozwoli na efektywną pracę z dowolnego miejsca.
- 1.3. Centralne przechowywanie poświadczeń i uprawnień: System powinien umożliwiać centralne zarządzanie tożsamościami użytkowników oraz ich uprawnieniami dostępu do zasobów firmy.
- 1.4. Integracja z istniejącymi systemami: Oprogramowanie musi być kompatybilne z obecnie używanymi systemami operacyjnymi i aplikacjami, aby zapewnić spójność działania.

**2. Wymagania techniczne.** Oprogramowanie powinno spełniać następujące wymagania techniczne:

- 2.1. Wsparcie dla protokołów zapewniających bezpieczne połączenie: System musi obsługiwać protokoły szyfrowania i autoryzacji, które zapewnią poufność i integralność przesyłanych danych.
- 2.2. Możliwość uruchamiania aplikacji zdalnie: Oprogramowanie powinno umożliwiać użytkownikom zdalne uruchamianie aplikacji, co pozwoli na elastyczną organizację pracy.
- 2.3. Centralne zarządzanie tożsamościami i dostępem użytkowników: System powinien umożliwiać centralne zarządzanie poświadczeniami i uprawnieniami użytkowników, co zwiększy bezpieczeństwo i efektywność zarządzania.



Fundusze Europejskie  
dla Łódzkiego



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



2.4. Kompatybilność z systemami operacyjnymi i aplikacjami używanymi w firmie:  
Oprogramowanie musi być kompatybilne z obecnie używanymi systemami operacyjnymi i aplikacjami, aby zapewnić spójność działania.

3. Licencje na zamawiany serwerowy system operacyjny muszą być bezterminowe.
4. Licencje muszą pochodzić z legalnego kanału dystrybucji na terenie kraju.
5. Bezpieczeństwo połączenia będzie zapewniane przez mechanizmy szyfrowania i autoryzacji, które gwarantują poufność i integralność przesyłanych danych. System powinien umożliwiać monitorowanie i audytowanie aktywności użytkowników, co pozwoli na szybkie wykrywanie i reagowanie na potencjalne zagrożenia. Dodatkowo, oprogramowanie powinno wspierać mechanizmy wieloskładnikowej autoryzacji (MFA), co zwiększy poziom bezpieczeństwa dostępu do zasobów firmy.