Załącznik nr 1 do SWZ

Nr postępowania: WIR.271.5.2025

**OPIS PRZEDMIOTU ZAMÓWIENIA – Zadanie 3 obszar techniczny**

**Pozycja 9. ROZWIĄZANIE DO BEZPIECZNEGO UDOSTĘPNIANIA DANYCH OSOBOWYCH WRAZ Z WDROŻENIEM – 1 kpl.**

WYMAGANIA SYSTEMOWE

1. Rozwiązanie "on premise"
2. Interfejs systemu dostępny w języku polskim.
3. Rozwiązanie w formie maszyny wirtualnej hostowanej lokalnie w infrastrukturze urzędu.
4. Rozwiązanie oparte na technologii Docker, umożliwiające łatwą skalowalność, elastyczność wdrożeń oraz optymalizację zasobów. Dzięki tej technologii system może być efektywnie zarządzany w środowisku kontenerowym, co upraszcza procesy konfiguracji, aktualizacji oraz migracji.
5. Rozwiązanie oparte na oprogramowaniu open source, bez konieczności ponoszenia opłat licencyjnych.
6. Zgodność z obowiązującymi standardami bezpieczeństwa informatycznego, wymaganiami RODO w zakresie ochrony danych osobowych oraz zabezpieczenie systemu przed nieautoryzowanym dostępem i wyciekiem danych.

WYMAGANIA FUNKCJONALNE

1. Dostarczenie i wdrożenie narzędzia informatycznego umożliwiającego bezpieczne i efektywne udostępnianie dokumentów poprzez Internet, opartego na rozwiązaniu open source dedykowanym do współdzielenia plików i współpracy. Rozwiązanie powinno być dostosowane do wymogów organizacji publicznej, zapewniając wysoki poziom ochrony danych i zgodność z obowiązującymi przepisami prawa.
2. System musi posiadać mechanizmy zabezpieczające przed atakami typu brute force, takie jak blokowanie adresów IP po określonej liczbie nieudanych prób logowania oraz możliwość ustawienia reguł ograniczających dostęp.
3. Administrator systemu musi mieć możliwość tworzenia i usuwania kont użytkowników oraz zarządzania ich uprawnieniami.
4. Możliwość połączenia z istniejącymi zasobami danych (np. systemami NAS).

BEZPIECZNE UDOSTĘPNIANIE DANYCH

1. Wsparcie dla uwierzytelniania dwuskładnikowego (2FA) w celu zabezpieczenia dostępu użytkowników.
2. Funkcja umożliwiająca udostępnianie plików i dokumentów zewnętrznym kooperantom z wykorzystaniem unikalnych linków zabezpieczonych hasłem.
3. Wymóg użycia połączeń szyfrowanych z wykorzystaniem certyfikatu SSL.
4. Ograniczenie czasowe udostępniania
5. Funkcjonalność określania czasu ważności linku do udostępnianych plików

OBSŁUGA DUŻYCH PLIKÓW

1. System musi umożliwiać przechowywanie i przesyłanie plików o wielkości nie mniejszej niż 100 MB.
2. Dostęp przez przeglądarkę internetową:
3. Pełna obsługa systemu przez interfejs webowy, bez konieczności instalowania dodatkowego oprogramowania.

BACKUP SYSTEMU

1. Automatyczny backup systemu kopia zapasowa danych z możliwością przywrócenia systemu w przypadku awarii.

AUDYT I LOGI

1. Rozwiązanie musi umożliwiać prowadzenie logów udostępniania dokumentów i aktywności użytkowników.

ZAKRES REALIZACJI I WYMAGANIA

1. Instalacja i konfiguracja oprogramowania.
2. Integracja z istniejącą infrastrukturą IT urzędu.
3. Szkolenie użytkowników oraz administratorów systemu.
4. Dostarczenie dokumentacji i instrukcji obsługi systemu w języku polskim.
5. Potwierdzone doświadczenie Wykonawcy w realizacji podobnych projektów oraz w zakresie wirtualizacji i ochrony danych osobowych.

WDROŻENIE I WSPARCIE

1. Przed rozpoczęciem wdrożenia wymagane jest przeprowadzenie wstępnego spotkania, na którym zostaną omówione wszystkie kroki procesu wdrożeniowego.
2. Przed docelowym uruchomieniem systemu wymagane jest przeprowadzenie testów integracyjnych i akceptacyjnych, aby upewnić się, że wszystkie elementy systemu działają poprawnie i są zgodne z wymaganiami zleceniodawcy.
3. Przed pełnym uruchomieniem zrealizowane zostanie przeszkolenie pracowników z obsługi nowego rozwiązania. Dostawca powinien zapewnić odpowiednie materiały szkoleniowe oraz warsztaty praktyczne.
4. Dostawca zobowiązany jest zapewnić ciągłe wsparcie techniczne w czasie pierwszych dni po wdrożeniu, aby szybko reagować na ewentualne problemy i pytania użytkowników końcowych.
5. Wdrożony system zostanie objęty 24-miesięczną gwarancją obejmującą szybkie reagowanie w przypadku awarii, bieżące aktualizacje oprogramowania oraz okresowe audyty weryfikujące wymagany poziom zabezpieczeń systemu w trakcie okresu wsparcia.
6. W okresie obowiązywania gwarancji zostanie zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.