*Załącznik nr 4a do SWZ*

**OPIS PRZEDMIOTU ZAMÓWIENIA  
do części 1  
Wdrożenie serwera logów**

w postępowaniu o udzielenie zamówienia publicznego w trybie podstawowym bez negocjacji o wartości zamówienia mniejszej niż kwoty określone w obwieszczeniu Prezesa Urzędu Zamówień Publicznych, ogłoszonym na podstawie art. 3 ust. 3 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tekst jednolity Dz.U. z 2022 r. poz. 1710 ze zm.), pod nazwą:

realizowanego w ramach projektu

**„Cyfrowa Gmina”**

**Zamawiający**: Gmina Skoczów, ul. Rynek 1, 43-430 Skoczów

## OPS ROZWIĄZANIA

Proponowany system, ma działać jako maszyn wirtualna Hyper-V oparta o darmowy serwer logów Greylog działającym w darmowym systemie operacyjnym Linux posiadającym wsparcie co najmniej do roku 2026. Oprócz funkcji zbierania i archiwizacji logów, zawierać ma szereg funkcjonalności usprawniających zarządzanie i monitorowanie infrastruktury informatycznej.

## KONCEPCJA WDROŻENIA

Wdrożenie centralnego systemu zbierania logów w wariancie obejmującym:

* 1. Opracowanie projektu,
  2. Przygotowanie systemu do pracy,
  3. Dołączenie określonych źródeł,
  4. Opracowanie procedur eksploatacyjnych (w tym dołączania kolejnych źródeł),
  5. Przeszkolenie Administratorów Zamawiającego.

## USŁUGI WDROŻENIOWE

Pełen zakres usług wdrożeniowych obejmuje:

1. Opracowanie projektu i harmonogramu prac wdrożeniowych, w tym:
   1. oszacowanie wymaganej ilości przestrzeni dyskowej na bieżące logi oraz dla archiwum,
   2. określenie parametrów wydajnościowych serwera na podstawie testów w środowisku produkcyjnym (CPU, RAM, IOPS).
2. Utworzenie struktury serwerowej systemu:
   1. instalacja serwera zbierającego logi jako maszyna wirtualna Hyper-V,
   2. instalacja darmowego systemu operacyjnego Linux,
   3. instalacja darmowego oprogramowania Graylog (w tym Java JDK, MongoDB, Elasticsearch lub OpenSearch).
3. Konfiguracja zabezpieczeń dostępu do systemu:
   1. uruchomienie autoryzacji Active Directory/LDAP,
   2. włączenie protokołu HTTPS,
   3. definicja ról dostępu do (AD/LDAP).
4. Konfiguracja i kalibracja systemu:
   1. zdefiniowanie startowej polityki rotacji i retencji logów,
   2. definicja szablonów konfiguracyjnych dla agentów zasilających system logami z systemów Linux/Windows,
   3. Ustawienie retencji logów na 24 miesiące,
   4. definicja wejść systemu dla grup urządzeń sieciowych,
   5. konfiguracja synchronizacji czasu: serwera zbierającego logi, źródeł logów.
5. Dołączenie źródeł syslog, w tym:
   1. logi UTM – 1 szt.
   2. logi przełączników sieciowych – 9 szt.
   3. logi sprzętowe serwerów fizycznych – 2 szt.
   4. logi sprzętowe macierzy – 1 szt. i serwerów NAS – 2 szt.
   5. logi stacji roboczych – min 3 szt.
6. Dołączenie źródeł systemowych i aplikacyjnych maszyn wirtualnych:
   1. logi systemowe i aplikacyjne Windows Server 2019 – 7 szt. (w tym zdarzenia związane z użytkownikami, takie jak autoryzacja użytkownika, zmiana hasła, audyt udostępnionego zasobu: modyfikacja plików, usuwanie plików, audyt zdarzeń dotyczących użytkowników oraz serwera)
      1. Kontrolery domeny AD
      2. Serwery plików w AD
      3. Serwery aplikacyjne
   2. logi systemowe Linux – 6szt. (w tym zdarzenia dotyczące użytkowników),
   3. logi serwera bazodanowego MSSQL Express.
7. Wdrożenie obróbki wstępnej logów i analizy logów.
8. Prezentacja danych na panelu w formie graficznej:
   1. ruchu na urządzeniach sieciowych,
   2. monitorowanie i audyt Active Directory (logowanie użytkowników, dostęp do plików),
   3. monitorowanie serwera www (intranet).
9. Uruchomienie 3 przykładowych alertów/działań proaktywnych dla zbieranych logów.
10. Testy prawidłowego funkcjonowania systemu.
11. Szkolenie administratora systemu w wymiarze 4 godzin.
12. Opracowanie dokumentacja powykonawczej, w tym:
    1. dokumentacji systemu,
    2. procedur eksploatacyjnych (m.in. dodawanie nowych urządzeń do serwera logów)

## WSPARCIE POWDROŻENIOWE

Minimum 180 dni bezpłatnego wsparcia powdrożeniowego w formie zdalnej, od dnia podpisania protokołu odbioru bez uwag.

Zakres wsparcia powdrożeniowego w formie zdalnej obejmować będzie:

1. Naprawa usterek związanych z prawidłowym przesyłaniem i rejestrowaniem logów z urządzeń i aplikacji.
2. Pomoc w konfiguracji nowych źródeł podłączanych do systemu Greylog.
3. Pomoc w konfiguracji paneli graficznych wizualizujących przetwarzane dane.
4. Pomoc w definiowaniu alarmów.
5. Pomoc w optymalizacji wydajności i zużywanych zasobów systemu Greylog.

## TERMIN WYKONANIA USŁUGI

Termin realizacji zamówienia – **do 30 dni** od daty podpisania umowy