

OPIS PRZEDMIOTU ZAMÓWIENIA

dla zadania

„Wdrożenie systemu monitorowania infrastruktury teleinformatycznej oraz systemu monitorowania cyberbezpieczeństwa w Zakładzie Gospodarki Wodno-Ściekowej w Słońsku wraz z integracją z centralnym systemem monitorowania Urzędu Gminy Słońsk”

1. Informacje ogólne

1.1 Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja, uruchomienie oraz wdrożenie systemu monitorowania infrastruktury teleinformatycznej oraz systemu monitorowania cyberbezpieczeństwa w Zakładzie Gospodarki Wodno-Ściekowej w Słońsku wraz z integracją z centralnym systemem monitorowania funkcjonującym w Urzędzie Gminy Słońsk.

Zakres zamówienia obejmuje wykonanie wszelkich dostaw, usług i prac niezbędnych do osiągnięcia funkcjonalności określonych w niniejszym Opisie Przedmiotu Zamówienia (OPZ), w szczególności:

- dostawę i instalację niezbędnych komponentów rozwiązania;
- konfigurację systemów monitorowania;
- konfigurację monitorowania urządzeń i usług;
- przeprowadzenie testów funkcjonalnych;
- integrację z centralnym systemem monitorowania;
- przekazanie dokumentacji powykonawczej;
- przeprowadzenie szkolenia administratorów;
- udzielenie gwarancji na wykonane prace.

1.2 Cel zamówienia

Celem zamówienia jest wdrożenie rozwiązania zapewniającego:

- monitorowanie infrastruktury teleinformatycznej;
- monitorowanie dostępności urządzeń i usług;
- centralizację logów z monitorowanych systemów;
- wykrywanie, analizę oraz prezentację zdarzeń związanych z cyberbezpieczeństwem;
- automatyczne alarmowanie o wykrytych zdarzeniach;
- integrację z centralnym systemem monitorowania Urzędu Gminy Słońsk.

Wdrożone rozwiązanie powinno umożliwiać Zamawiającemu samodzielną administrację oraz dalszą rozbudowę bez konieczności korzystania z usług Wykonawcy, z zastrzeżeniem przypadków wymagających odrębnych prac wdrożeniowych.

Dlaczego ta zmiana?

Dodałem ostatnie zdanie, ponieważ jasno określa ono jeden z głównych celów zamówienia – niezależność Zamawiającego po zakończeniu wdrożenia. Jednocześnie nie ogranicza możliwości zlecenia dodatkowych prac w przyszłości.

1.3 Rozwiązania równoważne

Ileć w niniejszym OPZ wskazano nazwę producenta, produktu, technologii lub rozwiązania, należy ją traktować wyłącznie jako określenie minimalnych wymagań funkcjonalnych, technicznych i jakościowych.

Zamawiający dopuszcza zastosowanie rozwiązań równoważnych, pod warunkiem że zapewniają one funkcjonalność, poziom bezpieczeństwa, wydajność, kompatybilność oraz możliwości integracji nie gorsze niż wymagane w niniejszym OPZ.

Wykonawca oferujący rozwiązanie równoważne zobowiązany jest wykazać jego równoważność poprzez przedstawienie dokumentacji technicznej lub innych dokumentów potwierdzających spełnienie wymagań określonych w OPZ.

1.4 Zasada kompletności rozwiązania

Wykonawca zobowiązany jest dostarczyć kompletne i w pełni funkcjonalne rozwiązanie spełniające wszystkie wymagania określone w niniejszym OPZ.

Jeżeli do prawidłowego działania rozwiązania niezbędne będzie zastosowanie dodatkowych komponentów, modułów, licencji, usług, konfiguracji lub innych elementów niewskazanych wprost w OPZ, Wykonawca zobowiązany jest uwzględnić je w cenie oferty.

W dniu podpisania protokołu odbioru końcowego wdrożone rozwiązanie musi być kompletne, skonfigurowane oraz gotowe do eksploatacji.

2. Opis środowiska Zamawiającego

2.1 Informacje ogólne

Środowisko teleinformatyczne Zamawiającego obejmuje infrastrukturę wykorzystywaną do realizacji zadań Zakładu Gospodarki Wodno-Ściekowej w Słońsku.

System monitorowania zostanie wdrożony w infrastrukturze eksploatowanej przez Zamawiającego i obejmie urządzenia oraz systemy wskazane do monitorowania na etapie realizacji zamówienia.

2.2 Zakres infrastruktury

Monitoring obejmie w szczególności:

- serwery fizyczne;
- serwery wirtualne;
- stacje robocze;
- urządzenia sieciowe;
- urządzenia UTM;
- urządzenia NAS;
- urządzenia UPS;
- urządzenia systemu monitoringu wizyjnego (CCTV);
- drukarki sieciowe;
- inne urządzenia wyposażone w mechanizmy umożliwiające monitorowanie ich stanu technicznego lub parametrów pracy.

2.3 Założenia wdrożenia

Wdrożenie należy przeprowadzić w sposób zapewniający ciągłość pracy Zamawiającego.

Prace mogące powodować przerwy w dostępności usług lub urządzeń wymagają wcześniejszego uzgodnienia z Zamawiającym.

Wykonawca zobowiązany jest ograniczyć wpływ prowadzonych prac na bieżące funkcjonowanie infrastruktury teleinformatycznej.

Jeżeli w trakcie realizacji prac wystąpi konieczność czasowego wyłączenia urządzeń lub usług, termin oraz sposób wykonania prac zostaną uzgodnione z Zamawiającym.

2.4 Dostęp do infrastruktury

Zamawiający zapewni Wykonawcy dostęp do infrastruktury w zakresie niezbędnym do realizacji przedmiotu zamówienia.

Zakres oraz sposób realizacji dostępu, w tym dostępu zdalnego, zostaną uzgodnione przed rozpoczęciem prac z uwzględnieniem obowiązujących u Zamawiającego zasad bezpieczeństwa.

Wykonawca zobowiązany jest korzystać wyłącznie z udostępnionych kanałów komunikacji oraz przyznanych uprawnień.

2.5 Stan środowiska

Przed rozpoczęciem konfiguracji rozwiązania Wykonawca zobowiązany jest zapoznać się ze środowiskiem teleinformatycznym Zamawiającego w zakresie niezbędnym do prawidłowej realizacji zamówienia.

W przypadku stwierdzenia okoliczności mogących mieć wpływ na realizację zamówienia lub osiągnięcie wymaganej funkcjonalności, Wykonawca niezwłocznie poinformuje o tym Zamawiającego oraz przedstawi propozycję sposobu ich usunięcia.

Na żądanie Zamawiającego Wykonawca przedłoży dokumentację techniczną, karty katalogowe lub inne dokumenty potwierdzające spełnienie wymagań określonych w OPZ, w tym równoważność oferowanego rozwiązania.

3. Wymagania dla systemu monitorowania infrastruktury

3.1 Wymagania ogólne

Wykonawca wdroży system monitorowania infrastruktury teleinformatycznej umożliwiający bieżący nadzór nad stanem urządzeń, usług oraz parametrów pracy infrastruktury Zamawiającego.

System musi:

- pracować w architekturze umożliwiającej jego dalszą rozbudowę bez konieczności wymiany podstawowych komponentów;
- udostępniać interfejs administracyjny dostępny z poziomu przeglądarki internetowej;
- umożliwiać jednoczesne monitorowanie wszystkich urządzeń objętych zakresem zamówienia;
- umożliwiać samodzielną administrację przez Zamawiającego po zakończeniu wdrożenia.

3.2 Zakres monitorowania

System musi umożliwiać monitorowanie co najmniej:

- serwerów fizycznych;
- serwerów wirtualnych;
- stacji roboczych;
- urządzeń sieciowych;
- urządzeń UTM;
- urządzeń NAS;
- urządzeń UPS;
- urządzeń systemu monitoringu wizyjnego (CCTV);
- drukarek sieciowych;
- innych urządzeń wskazanych przez Zamawiającego.

3.3 Metody monitorowania

System musi umożliwiać monitorowanie z wykorzystaniem metod odpowiednich do monitorowanego urządzenia lub usługi, w szczególności:

- ICMP;
- SNMP v2c i SNMP v3;
- agentów monitorujących;
- Syslog;
- interfejsów API;
- innych standardowych mechanizmów zapewniających równoważną funkcjonalność.

Dobór metody monitorowania pozostaje po stronie Wykonawcy.

Jeżeli monitorowane urządzenie obsługuje kilka metod komunikacji, Wykonawca dobierze rozwiązanie zapewniające możliwie największy zakres monitorowanych parametrów.

3.4 Monitorowane parametry

System musi umożliwiać monitorowanie co najmniej:

- dostępności urządzeń;
- dostępności usług;
- obciążenia procesora;
- wykorzystania pamięci operacyjnej;
- wykorzystania przestrzeni dyskowej;
- stanu macierzy RAID;
- stanu dysków;
- temperatur;
- pracy wentylatorów;
- stanu zasilaczy;
- parametrów interfejsów sieciowych;
- wykorzystania przepustowości;
- czasu odpowiedzi.

Jeżeli urządzenie udostępnia dodatkowe parametry diagnostyczne, system powinien umożliwiać ich monitorowanie po konfiguracji przez administratora.

3.5 Alarmowanie

System musi umożliwiać definiowanie progów alarmowych oraz automatyczne generowanie alarmów po wystąpieniu zdefiniowanych zdarzeń.

Alarmy powinny obejmować co najmniej:

- niedostępność urządzenia;
- niedostępność usługi;
- przekroczenie progów wykorzystania procesora;
- przekroczenie progów wykorzystania pamięci;
- zapełnienie przestrzeni dyskowej;
- awarię macierzy RAID;
- awarię zasilania UPS;
- utratę komunikacji sieciowej;
- inne zdarzenia zdefiniowane przez administratora.

Administrator musi mieć możliwość samodzielnego definiowania oraz modyfikowania progów alarmowych.

3.6 Powiadomienia

System musi umożliwiać wysyłanie powiadomień o zdarzeniach co najmniej za pomocą:

- poczty elektronicznej;
- webhooków;
- interfejsów API.

Konfiguracja sposobu powiadamiania musi być dostępna dla administratora.

3.7 Wizualizacja danych

System musi umożliwiać tworzenie dashboardów prezentujących w szczególności:

- stan infrastruktury;
- aktywne alarmy;
- historię zdarzeń;
- wykorzystanie zasobów;
- dostępność urządzeń;

- trendy wydajności.

Administrator musi mieć możliwość samodzielnego tworzenia oraz modyfikowania dashboardów.

3.8 Raportowanie

System musi umożliwiać generowanie raportów obejmujących co najmniej:

- dostępność urządzeń;
- historię alarmów;
- wykorzystanie zasobów;
- trendy wydajności.

Raporty muszą umożliwiać eksport do formatów PDF oraz XLSX lub CSV.

3.9 Zarządzanie

Administrator musi mieć możliwość:

- dodawania i usuwania urządzeń;
- grupowania urządzeń;
- przypisywania szablonów monitorowania;
- importu i eksportu konfiguracji;
- wykonywania oraz odtwarzania kopii bezpieczeństwa konfiguracji;
- zarządzania użytkownikami oraz ich uprawnieniami.

3.10 Dokumentacja

Po zakończeniu wdrożenia Wykonawca przekaże:

- konfigurację systemu umożliwiającą jej ponowne wykorzystanie;
- zastosowane szablony monitorowania;
- utworzone dashboardy;
- instrukcję administratora;
- procedurę wykonywania i odtwarzania kopii bezpieczeństwa.

4. Wymagania dla systemu monitorowania cyberbezpieczeństwa

4.1 Wymagania ogólne

Wykonawca wdroży system monitorowania cyberbezpieczeństwa umożliwiający centralne gromadzenie, analizę oraz korelację zdarzeń bezpieczeństwa pochodzących z monitorowanych urządzeń i systemów.

System musi:

- umożliwiać wykrywanie incydentów bezpieczeństwa;
- identyfikować podatności występujące w monitorowanych systemach;
- monitorować zmiany mające wpływ na bezpieczeństwo środowiska teleinformatycznego;
- udostępniać interfejs administracyjny dostępny z poziomu przeglądarki internetowej;
- umożliwiać samodzielną administrację przez Zamawiającego po zakończeniu wdrożenia.

4.2 Zakres monitorowania i pozyskiwania zdarzeń

System musi umożliwiać monitorowanie oraz pozyskiwanie zdarzeń bezpieczeństwa z urządzeń i systemów objętych zakresem zamówienia, w szczególności z:

- serwerów z systemem Windows;
- stacji roboczych;
- serwerów z systemem Linux, jeżeli występują w środowisku Zamawiającego;
- urządzeń UTM;
- urządzeń sieciowych;
- urządzeń NAS;
- urządzeń UPS;
- rejestratorów systemów monitoringu wizyjnego (CCTV), jeżeli udostępniają logi lub zdarzenia;
- innych urządzeń i systemów teleinformatycznych wskazanych przez Zamawiającego.

Pozyskiwanie danych musi być realizowane z wykorzystaniem mechanizmów odpowiednich do monitorowanego urządzenia lub systemu, w szczególności poprzez:

- agentów monitorujących;
- protokół Syslog;
- protokół SNMP;
- mechanizmy agentless;
- protokoły WMI oraz SSH;
- interfejsy API;
- inne standardowe mechanizmy zapewniające równoważną funkcjonalność.

Dobór metody pozyskiwania danych pozostaje po stronie Wykonawcy.

Jeżeli monitorowane urządzenie nie umożliwia instalacji agenta, Wykonawca zastosuje inną metodę pozyskiwania danych zapewniającą możliwie najszerszy zakres monitorowania.

System musi umożliwiać jednoczesne wykorzystanie różnych metod pozyskiwania danych, odpowiednio do charakterystyki monitorowanych urządzeń i systemów.

Niezależnie od zastosowanej metody pozyskiwania danych system musi zapewniać:

- centralne gromadzenie zdarzeń;
- normalizację danych;
- korelację zdarzeń pochodzących z różnych źródeł;
- wyszukiwanie i filtrowanie zgromadzonych danych;
- prezentację zdarzeń w jednolitym interfejsie administracyjnym;
- wykorzystanie pozyskanych danych do monitorowania, alarmowania oraz raportowania.

4.3 Centralizacja logów

System musi zapewniać:

- centralne gromadzenie logów;
- indeksowanie i wyszukiwanie danych;
- filtrowanie zdarzeń;
- archiwizację logów;
- eksport danych.

Okres przechowywania logów zostanie ustalony z Zamawiającym z uwzględnieniem dostępnych zasobów infrastruktury oraz potrzeb eksploatacyjnych.

4.4 Analiza i korelacja zdarzeń

System musi umożliwiać:

- analizę zdarzeń bezpieczeństwa;
- korelację logów pochodzących z różnych źródeł;
- wykrywanie anomalii;
- identyfikację incydentów bezpieczeństwa;
- definiowanie własnych reguł analizy.

4.5 Monitorowanie integralności plików

System musi umożliwiać monitorowanie zmian integralności wskazanych plików i katalogów.

Monitorowanie powinno obejmować co najmniej:

- utworzenie pliku;
- usunięcie pliku;
- zmianę zawartości;
- zmianę uprawnień;
- zmianę właściciela.

Zakres monitorowanych lokalizacji zostanie uzgodniony z Zamawiającym podczas wdrożenia.

4.6 Wykrywanie podatności

System musi umożliwiać identyfikację podatności bezpieczeństwa występujących w monitorowanych systemach.

Dla wykrytych podatności powinny być prezentowane co najmniej:

- identyfikator podatności zgodny z powszechnie stosowanymi bazami (np. CVE);
- poziom ryzyka;
- opis podatności;
- zalecane działania naprawcze.

4.7 Alarmowanie

System musi automatycznie generować alarmy dotyczące co najmniej:

- prób nieautoryzowanego dostępu;
- wielokrotnych nieudanych prób logowania;
- zmian konfiguracji systemów;
- naruszenia integralności monitorowanych plików;
- wykrytych podatności;
- wykrycia złośliwego oprogramowania, jeżeli funkcjonalność jest dostępna;
- innych zdarzeń zdefiniowanych przez administratora.

Administrator musi mieć możliwość definiowania oraz modyfikowania reguł alarmowania.

4.8 Wizualizacja danych

System musi umożliwiać tworzenie dashboardów prezentujących w szczególności:

- aktywne incydenty;
- poziom zagrożeń;
- historię zdarzeń;

- wykryte podatności;
- stan monitorowanych agentów;
- trendy bezpieczeństwa.

Administrator musi mieć możliwość samodzielnego tworzenia i modyfikowania dashboardów.

4.9 Zarządzanie

Administrator musi mieć możliwość:

- instalowania i usuwania agentów;
- grupowania monitorowanych urządzeń;
- zarządzania konfiguracją;
- wykonywania oraz odtwarzania kopii bezpieczeństwa konfiguracji;
- importu i eksportu konfiguracji;
- zarządzania użytkownikami oraz ich uprawnieniami.

4.10 Aktualizacje

Na dzień odbioru końcowego wszystkie komponenty rozwiązania muszą pracować w aktualnych, stabilnych wersjach objętych wsparciem producenta lub społeczności rozwijającej dane rozwiązanie.

Wykonawca prześle procedurę aktualizacji systemu.

4.11 Licencjonowanie

Jeżeli oferowane rozwiązanie wymaga licencji, Wykonawca zapewni wszystkie licencje niezbędne do prawidłowego działania systemu przez okres wymagany dokumentacją zamówienia.

W przypadku zastosowania oprogramowania Open Source Wykonawca prześle informacje dotyczące wykorzystanych komponentów oraz warunków ich licencjonowania.

4.12 Dokumentacja

Po zakończeniu wdrożenia Wykonawca prześle:

- konfigurację systemu umożliwiającą jej ponowne wykorzystanie;
- dokumentację powykonawczą;
- instrukcję administratora;
- procedurę aktualizacji;
- procedurę wykonywania i odtwarzania kopii bezpieczeństwa.

5. Integracja oraz wymagania techniczne rozwiązania

5.1 Integracja z centralnym systemem monitorowania

Wdrożone rozwiązanie musi zostać zintegrowane z centralnym systemem monitorowania funkcjonującym w Urzędzie Gminy Słońsk.

Integracja musi umożliwiać przekazywanie informacji o zdarzeniach, alarmach oraz stanie monitorowanych systemów zgodnie z wymaganiami Zamawiającego.

Zakres wymienianych danych oraz sposób integracji zostaną uzgodnione z Zamawiającym na etapie realizacji zamówienia.

5.2 Wymagania komunikacyjne

Komunikacja pomiędzy komponentami wdrażanego rozwiązania powinna odbywać się z wykorzystaniem bezpiecznych protokołów transmisji danych.

Jeżeli wykorzystywane są mechanizmy szyfrowania, powinny być oparte na aktualnie wspieranych standardach.

Rozwiązanie nie może wymagać stosowania protokołów lub mechanizmów uznanych za przestarzałe albo powszechnie uznawanych za niebezpieczne, o ile ich użycie nie wynika z ograniczeń monitorowanego urządzenia.

5.3 Synchronizacja czasu

Wszystkie komponenty wdrażanego rozwiązania powinny wykorzystywać wspólne źródło czasu.

Synchronizacja czasu powinna odbywać się z wykorzystaniem usługi NTP lub równoważnego mechanizmu zapewniającego spójność znaczników czasu.

5.4 Zarządzanie użytkownikami

System musi umożliwiać tworzenie kont użytkowników oraz przypisywanie im uprawnień zgodnie z pełnionymi rolami.

Uprawnienia użytkowników powinny być nadawane zgodnie z zasadą minimalnych niezbędnych uprawnień.

Administrator musi mieć możliwość:

- tworzenia i usuwania kont użytkowników;
- blokowania i odblokowywania kont;
- zmiany uprawnień;
- przypisywania użytkowników do ról lub grup.

5.5 Rejestrowanie działań administracyjnych

System musi rejestrować działania wykonywane przez użytkowników posiadających uprawnienia administracyjne.

Rejestrowane powinny być co najmniej:

- logowanie i wylogowanie;
- zmiany konfiguracji;
- tworzenie i usuwanie kont;
- zmiany uprawnień;
- dodawanie i usuwanie monitorowanych urządzeń.

5.6 Kopie bezpieczeństwa konfiguracji

System musi umożliwiać wykonywanie kopii bezpieczeństwa konfiguracji.

Administrator musi mieć możliwość samodzielnego:

- wykonania kopii konfiguracji;
- odtworzenia konfiguracji;
- eksportu kopii bezpieczeństwa.

5.7 Wydajność rozwiązania

Wdrożone rozwiązanie powinno zapewniać stabilną pracę przy monitorowaniu wszystkich urządzeń objętych zakresem zamówienia.

Monitorowanie infrastruktury nie może powodować zauważalnego pogorszenia wydajności monitorowanych urządzeń.

5.8 Skalowalność

Rozwiązanie powinno umożliwiać rozbudowę o kolejne urządzenia oraz usługi bez konieczności wymiany podstawowych komponentów systemu.

Rozbudowa systemu nie może powodować utraty dotychczas zgromadzonych danych ani konieczności ponownej konfiguracji całego środowiska.

5.9 Gwarancja i wsparcie

Wykonawca zapewni gwarancję na wykonane prace wdrożeniowe zgodnie z warunkami określonymi w dokumentacji postępowania.

W okresie gwarancji Wykonawca zobowiązany jest do usuwania wad wynikających z niewłaściwego wykonania przedmiotu zamówienia.

5.10 Szkolenie

Po zakończeniu wdrożenia Wykonawca przeprowadzi szkolenie administratorów wskazanych przez Zamawiającego.

Szkolenie powinno obejmować co najmniej:

- administrację systemem;
- konfigurację monitorowania;
- obsługę alarmów;
- tworzenie raportów;
- wykonywanie kopii bezpieczeństwa;
- podstawowe czynności eksploatacyjne.

5.11 Dokumentacja powykonawcza

Po zakończeniu wdrożenia Wykonawca przekaze dokumentację powykonawczą obejmującą co najmniej:

- opis architektury wdrożonego rozwiązania;
- opis zastosowanej konfiguracji;
- wykaz monitorowanych urządzeń;
- wykaz zastosowanych komponentów;
- instrukcję administracyjną;
- instrukcję wykonywania aktualizacji;
- procedurę wykonywania i odtwarzania kopii bezpieczeństwa.

6. Wymagania dotyczące realizacji zamówienia

6.1 Termin realizacji

Przedmiot zamówienia zostanie zrealizowany w terminie określonym w dokumentacji postępowania.

Za termin zakończenia realizacji zamówienia uznaje się dzień podpisania protokołu odbioru końcowego bez zastrzeżeń lub zgodnie z postanowieniami umowy.

6.2 Organizacja prac

Prace wdrożeniowe będą prowadzone w uzgodnieniu z Zamawiającym, z uwzględnieniem konieczności zachowania ciągłości działania infrastruktury teleinformatycznej.

Wykonawca zobowiązany jest do uzgadniania z Zamawiającym terminów prac mogących powodować ograniczenie dostępności usług lub urządzeń.

6.3 Obowiązki Wykonawcy

Do obowiązków Wykonawcy należy w szczególności:

- dostarczenie wszystkich elementów niezbędnych do realizacji przedmiotu zamówienia;
- instalacja i konfiguracja wdrażanych rozwiązań;
- przeprowadzenie testów funkcjonalnych przed zgłoszeniem gotowości do odbioru;
- usunięcie stwierdzonych nieprawidłowości powstałych z przyczyn leżących po stronie Wykonawcy;
- przekazanie dokumentacji powykonawczej;
- przeprowadzenie szkolenia administratorów.

6.4 Wymagania dotyczące dokumentacji

Dokumentacja przekazywana Zamawiającemu powinna być sporządzona w języku polskim w postaci elektronicznej, a na żądanie Zamawiającego również w postaci papierowej.

Dokumentacja powinna być kompletna, aktualna oraz umożliwiać samodzielną eksploatację wdrożonego rozwiązania.

6.5 Gwarancja

Wykonawca udzieli gwarancji na wykonane prace oraz dostarczone elementy rozwiązania zgodnie z warunkami określonymi w dokumentacji postępowania oraz umowie.

W okresie gwarancji Wykonawca zobowiązany jest do usuwania wad wynikających z niewłaściwego wykonania przedmiotu zamówienia.

6.6 Wsparcie po wdrożeniu

Jeżeli dokumentacja postępowania przewiduje świadczenie wsparcia po zakończeniu wdrożenia, Wykonawca będzie realizował je na zasadach określonych w umowie.

7. Odbiór przedmiotu zamówienia

7.1 Warunki zgłoszenia do odbioru

Po zakończeniu realizacji przedmiotu zamówienia Wykonawca zgłosi Zamawiającemu gotowość do odbioru końcowego.

Zgłoszenie gotowości do odbioru może nastąpić po zakończeniu wszystkich prac objętych przedmiotem zamówienia, w szczególności po:

- dostawie i uruchomieniu wszystkich komponentów rozwiązania;
- zakończeniu konfiguracji systemów;
- wykonaniu integracji z centralnym systemem monitorowania;
- przeprowadzeniu testów funkcjonalnych przez Wykonawcę;
- przekazaniu dokumentacji powykonawczej;
- przeprowadzeniu szkolenia administratorów.

7.2 Odbiór końcowy

Odbiór końcowy zostanie przeprowadzony przez przedstawicieli Zamawiającego w obecności Wykonawcy.

Celem odbioru jest potwierdzenie zgodności wykonanego przedmiotu zamówienia z wymaganiami określonymi w OPZ oraz zawartą umową.

7.3 Testy odbiorowe

W ramach odbioru końcowego Zamawiający przeprowadzi testy odbiorowe potwierdzające spełnienie wymagań określonych w niniejszym OPZ.

Zakres testów odbiorowych określa **Załącznik nr 1 – Scenariusze testów odbiorowych**.

Wykonawca zobowiązany jest zapewnić udział osób posiadających wiedzę niezbędną do przeprowadzenia testów oraz udzielać wyjaśnień dotyczących działania wdrożonego rozwiązania.

7.4 Wynik odbioru

Jeżeli w trakcie odbioru zostaną stwierdzone wady lub niezgodności uniemożliwiające prawidłową eksploatację rozwiązania lub świadczące o niespełnieniu wymagań określonych w OPZ, Zamawiający może odmówić dokonania odbioru do czasu ich usunięcia.

Po usunięciu stwierdzonych wad lub niezgodności Wykonawca ponownie zgłosi gotowość do odbioru.

7.5 Protokół odbioru

Z przeprowadzonego odbioru zostanie sporządzony protokół odbioru podpisany przez przedstawicieli Zamawiającego i Wykonawcy.

Wzór protokołu odbioru stanowi **Załącznik nr 2 do OPZ**.

7.6 Kryteria uznania zamówienia za wykonane

Za wykonane uznaje się zamówienie, jeżeli łącznie zostały spełnione następujące warunki:

- wykonano wszystkie elementy przedmiotu zamówienia określone w OPZ;
- wdrożone rozwiązanie spełnia wymagania funkcjonalne i techniczne określone w OPZ;
- zakończono z wynikiem pozytywnym testy odbiorowe;
- przekazano wymaganą dokumentację;
- przeprowadzono szkolenie administratorów;
- podpisano protokół odbioru zgodnie z postanowieniami umowy.

Załącznik nr 1 do OPZ

Scenariusze testów odbiorowych

Lp.	Zakres testu	Sposób weryfikacji	Kryterium pozytywnego wyniku	Wynik
1	Instalacja i uruchomienie systemów	Weryfikacja działania wszystkich komponentów rozwiązania	Wszystkie komponenty zostały uruchomione i działają poprawnie	☐ P ☐ N
2	Monitoring infrastruktury	Sprawdzenie monitorowania urządzeń wdrożeniem	System prezentuje bieżący stan monitorowanych urządzeń	☐ P ☐ N
3	Monitoring cyberbezpieczeństwa	Weryfikacja odbioru i analizy zdarzeń bezpieczeństwa	Zdarzenia są poprawnie rejestrowane i prezentowane	☐ P ☐ N
4	Alarmowanie	Wywołanie zdarzenia testowego	System wygenerował alarm zgodnie z konfiguracją	☐ P ☐ N
5	Powiadomienia	Weryfikacja wysłania powiadomienia	Powiadomienie zostało dostarczone zgodnie z konfiguracją	☐ P ☐ N
6	Centralizacja logów	Weryfikacja odbioru logów z monitorowanych systemów	Logi są poprawnie odbierane i dostępne w systemie	☐ P ☐ N
7	Dashboardy	Weryfikacja prezentacji danych	Dashboardy prezentują aktualne dane	☐ P ☐ N
8	Raportowanie	Wygenerowanie raportu	Raport został wygenerowany zgodnie z wymaganiami OPZ	☐ P ☐ N
9	Zarządzanie użytkownikami	Sprawdzenie możliwości zarządzania	Administrator może zarządzać użytkownikami	☐ P ☐ N

		kontami i uprawnieniami	zgodnie z nadanymi uprawnieniami	
10	Kopia bezpieczeństwa konfiguracji	Wykonanie kopii konfiguracji	Kopia została wykonana bez błędów	☐ P ☐ N
11	Integracja z centralnym systemem monitorowania	Weryfikacja wymiany danych	Integracja działa zgodnie z wymaganiami OPZ	☐ P ☐ N
12	Dokumentacja powykonawcza	Sprawdzenie kompletności dokumentacji	Dokumentacja została przekazana zgodnie z OPZ	☐ P ☐ N
13	Szkolenie administratorów	Potwierdzenie przeprowadzenia szkolenia	Szkolenie zostało przeprowadzone zgodnie z OPZ	☐ P ☐ N

Wynik testów odbiorowych

Wynik	Wynik
Pozytywny	☐
Negatywny	☐

Uwagi

.....

.....

.....

.....

Wnioski końcowe

- ☐ Wszystkie testy zakończyły się wynikiem pozytywnym.
- ☐ Stwierdzono niezgodności wymagające usunięcia przed odbiorem końcowym.
- ☐ Odbiór końcowy został zakończony wynikiem pozytywnym.
- ☐ Odbiór końcowy został zakończony wynikiem negatywnym.

10. Podpisy

Ze strony Zamawiającego

Imię i nazwisko	Funkcja	Podpis

Ze strony Wykonawcy

Imię i nazwisko	Funkcja	Podpis

Załącznik nr 2 do OPZ

PROTOKÓŁ ODBIORU KOŃCOWEGO

dotyczący realizacji zamówienia pn.:

„Wdrożenie systemu monitorowania infrastruktury teleinformatycznej oraz systemu monitorowania cyberbezpieczeństwa w Zakładzie Gospodarki Wodno-Ściekowej w Słōnsku wraz z integracją z centralnym systemem monitorowania Urzędu Gminy Słōnsk”

1. Dane odbioru

Data odbioru:

Miejsce odbioru:

2. Strony uczestniczące w odbiorze

Zamawiający

Zakład Gospodarki Wodno-Ściekowej w Słōnsku

Przedstawiciele:

1.
2.

Wykonawca

Nazwa:

.....

Przedstawiciele:

1.
2.

3. Zakres odbioru

Przedmiotem odbioru jest realizacja zamówienia obejmującego:

- ☐ dostawę komponentów rozwiązania
- ☐ instalację i konfigurację systemu monitorowania infrastruktury

- ☐ instalację i konfigurację systemu monitorowania cyberbezpieczeństwa
- ☐ integrację z centralnym systemem monitorowania
- ☐ przeprowadzenie testów funkcjonalnych
- ☐ przekazanie dokumentacji powykonawczej
- ☐ przeprowadzenie szkolenia administratorów

4. Wynik testów odbiorowych

Na podstawie przeprowadzonych testów odbiorowych, wykonanych zgodnie z **Załącznikiem nr 1 do OPZ – Scenariusze testów odbiorowych**, komisja stwierdza:

- ☐ Wszystkie testy zakończyły się wynikiem pozytywnym.
- ☐ Stwierdzono niezgodności opisane w pkt 5 niniejszego protokołu.

5. Stwierdzone niezgodności / uwagi

.....

.....

.....

.....

.....

6. Dokumentacja przekazana przez Wykonawcę

- ☐ Dokumentacja powykonawcza
- ☐ Instrukcja administratora
- ☐ Procedura wykonywania i odtwarzania kopii bezpieczeństwa
- ☐ Procedura aktualizacji systemu
- ☐ Inne:

7. Decyzja komisji odbiorowej

Po przeprowadzeniu odbioru komisja postanawia:

- ☐ odebrać przedmiot zamówienia bez zastrzeżeń;
- ☐ odebrać przedmiot zamówienia z zastrzeżeniami;
- ☐ odmówić odbioru do czasu usunięcia stwierdzonych niezgodności.

8. Termin usunięcia niezgodności (jeżeli dotyczy)

.....

.....

9. Postanowienia końcowe

Z dniem podpisania niniejszego protokołu:

- Wykonawca potwierdza wykonanie przedmiotu zamówienia w zakresie określonym w umowie i OPZ.
- Zamawiający potwierdza wykonanie odbioru zgodnie z niniejszym protokołem, z uwzględnieniem decyzji wskazanej w pkt 7.

10. Podpisy

Ze strony Zamawiającego

Imię i nazwisko	Funkcja	Podpis

Ze strony Wykonawcy

Imię i nazwisko	Funkcja	Podpis