**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Uwaga: Zamawiający nie posiada kodów źródłowych do systemu SAOL. Kody źródłowe są w posiadaniu Wykonawcy SCH Elektronik Sławomir Chwałowski, ul. Sportowa 35, 97-300 Piotrków Trybunalski.**

SAOL – System Alarmowania i Ostrzegania Ludności – jest to system webowy do zarządzania systemami alarmowania i ostrzegania ludności. Innowacyjne rozwiązania zastosowane w oprogramowaniu SAOL pozwalają jednostkom zarzadzania kryzysowego w pełni monitorować w czasie rzeczywistym punkty alarmowe. Celem systemu jest ochrona życia.

Przedmiotem zamówienia jest:

1. Wykonanie usługi programistycznej polegającej na optymalizacji Web API SAOL MUW pod katem zapytań do bazy danych w celu przyspieszenia działania interfejsu graficznego użytkownika Systemu SAOL (na środowisku produkcyjnym);
2. Wykonanie usługi programistycznej polegającej na aktualizacji i rozbudowie dedykowanego oprogramowania serwera VPN działającego na potrzeby łączności Systemu SAOL, który ma być w pełni kompatybilny z istniejącym serwerem API;
3. W ramach udzielonej gwarancji na wykonane prace programistyczne wskazane w punktach 1 i 2 powyżej, Wykonawca udzieli bezpłatnego wsparcia serwisowego w ilości 50 godzin w zakresie:
4. administrowania Web API SAOL MUW w środowisku testowym
i produkcyjnym;
5. oprogramowania serwera VPN w środowisku produkcyjnym;
6. integracji z systemami podległymi Zamawiającego;
7. udzielania konsultacji przedstawicielom Zamawiającego.

**Ad. 1. Wykonanie usługi programistycznej polegającej na optymalizacji Web API SAOL MUW pod katem zapytań do bazy danych w celu przyspieszenia działania interfejsu graficznego użytkownika Systemu SAOL (na środowisku produkcyjnym), polegać będzie na:**

- Przyspieszeniu działania interfejsu graficznego użytkownika systemu SAOL, w ten sposób aby czas od momentu włączenia przycisku „włącz syreny” do rozdystrybuowania sygnału uruchomienia syren
z centrali wojewódzkiej do Punktów Alarmowych nie był dłuższy niż 3 sekundy.

- Wykonaniu sprawdzenia tabel pod kątem poprawności zapisu na nośniku, w rezultacie czego nastąpi zwolnienie zbędnych ilości danych na nośniku.

- Aktualizacji widoku w zakładce TABLICA i SYRENY – wszystkie dane mają być przechowywane w tabeli bazy danych zbiorczych, tabela ta ma aktualizować się raz na dobę po testach dobowych systemów powiatowych i gminnych. Aktualizacja danych zbiorczych musi również być możliwa na żądanie administratora systemu, proces ten ma być możliwy do uruchomienia z poziomu interfejsu graficznego użytkownika za pomocą dedykowanego przycisku.

- Dodaniu zakładki URUCHOM ALARM. Zakładka ma mieć umożliwiać szybkiego uruchomienia alarmów w wybranych powiatach. Widok ma być pozbawiony zbędnych statystycznych danych systemów podrzędnych, ma służyć jedynie do szybkiego reagowania w razie zagrożenia. W widoku szybkiego reagowania URUCHOM ALARM musi być widoczna zbiorcza kondycja systemu bez danych szczegółowych.

- Aktualizacji algorytmów uruchomienia alarmów musi odbywać się w sposób strukturalny, w pierwszej kolejności algorytmy muszą nadawać sygnał uruchomienia alarmów do Podsystemów Powiatowych,
w następnej kolejności do Podsystemów Gminnych w następnej kolejności bezpośrednio do Punktów Alarmowych.

- Wykonaniu modernizacji aktualizacji wysyłania żądań uruchomieniowych do central podrzędnych
z żądań synchronicznych na asynchroniczne w protokole komunikacyjnym TCP.

- Rozbudowie protokołu komunikacyjnego Web API SAOL MUW poprzez dodanie funkcjonalności uruchomienia alarmów i komunikatów w Systemie SAOL w trybie cichym. Tryb ten powinien mieć możliwość włączania alarmów i komunikatów w celu sprawdzenia skuteczności uruchomienia Systemu SAOL w sytuacjach krytycznych w przypadku utraty jednego z mediów sterujących (jest ich co najmniej dwa) w danym momencie.

**Ad. 2. Wykonanie usługi programistycznej polegającej na aktualizacji
i rozbudowie dedykowanego oprogramowania serwera VPN działającego na potrzeby łączności Systemu SAOL, który ma być w pełni kompatybilny
z istniejącym serwerem API, obejmować będzie:**

- Wykonaniu aktualizacji dedykowanego oprogramowania, której celem będzie przydzielanie statycznych adresów IP dla nowych klientów w sieci VPN z webowego interfejsu użytkownika dla serwera [saolvpn.mazowieckie.pl](http://saolvpn.mazowieckie.pl/). Aktualizacja danego oprogramowania musi być kompatybilna wstecznie i nie może wpłynąć na zmianę dotychczasowej adresacji  IP w istniejącej sieci VPN.

- Wykonaniu aktualizacji pakietówOpenVPN – przez podniesienie wersji VPN 2.1.4. do wersji 2.2.1.

- Rozbudowie programistycznej, której podlegać mają wszystkie warstwy programistyczne wymagane do prawidłowego funkcjonowania serwera VPN po aktualizacji. Rozbudowie, aktualizacji i konfiguracji mają podlegać: baza danych, kontrolery, modele, widoki, algorytmy oraz pakiet OpenVPN. Zamawiający określa prawidłową pracę serwera VPN w momencie stwierdzenia bezbłędnego wdrożenia wszystkich funkcjonalności opisanych w tym dokumencie/w tym OPZ, a w szczególności funkcjonalności ręcznej adresacji IP klientów serwera VPN. Wykonawca zobowiązany jest do aktualizacji webowego interfejsu graficznego w zakresie niezbędnym do prawidłowej obsługi systemu tj. skutecznego uruchomienia alarmów w systemie przez administratora/operatora dedykowanego systemu serwera VPN.

- Wykonawca zobowiązany jest do wdrożenia nowej zakładki, która będzie posiadać widok strukturalny połączeń VPN w systemie. Struktura systemu ma przedstawiać połączenia VPN
w postaci „drzewa”, grupowanego „nazwami” powiatów. Po naciśnięciu nazwy powiatu lub dedykowanego przycisku ma rozwijać się lista urządzeń podłączonych do danego powiatu. Na liście musi znajdować się nazwa klucza VPN oraz opis punktu Alarmowego. Dodatkowo na liście musi znajdować się adres IP danego klucza VPN w następujących opcjach:

- kolor zielony – połączenie sprawne
- kolor czerwony – brak połączenia
- kolor szary – urządzenie nie posiada interfejsu do sterowania po WAN/INTERNET.

 - Wykonawca musi przeprowadzić integrację z centralą wojewódzką produkcyjną MUW i zapasową w zakresie pozyskania danych na temat punktów alarmowych, w celu pobrania informacji na temat medium sterowania danego punktu alarmowego (LAN;RADIO;LAN/RADIO).

- Pobieranie danych musi odbywać się cyklicznie raz na dobę. Wykonawca zobowiązany jest do stworzenia, wdrożenia i dostarczenia API po dwóch stronach systemu, tj. w oprogramowaniu centrali wojewódzkiej produkcyjnej i zapasowej SAOL MUW producenta SCH ELEKTRONIK oraz
w dedykowanym oprogramowaniu serwera VPN MUW.

- Wykonawca musi przeprowadzić aktualizację bazy danych w zakresie: rozszerzenia tabeli bazy danych o informacje na temat punktu alarmowego o adres IP urządzenia i medium sterowania Punktu Alarmowego.

- Wykonawca dokona wdrożenia modułu automatycznego raportowania o stanie systemu VPN drogą mailową na wyznaczone przez administratora w systemie adresy użytkowników. Adresy IP muszą zostać pobrane z konfiguracji serwera OPENVPN i zostać wprowadzone do bazy danych. Adresacja IP musi być zsynchronizowana po nazwie klucza VPN. Usunięcie klucza VPN z listy musi spowodować usunięcie i zablokowania klucza, aby w przyszłości nie miał dostępu do sieci VPN.

- Wykonawca usunie zakładkę "Lista stałych adresów IP", która nie jest już kompatybilna
z istniejącą konfiguracją serwera VPN. Wykonawca zobligowany jest do wprowadzenia możliwości przeadresowywania IP Punktów Alarmowych z poziomu interfejsu graficznego. Administrator systemu musi mieć możliwość ręcznej zmiany adresów IP dla urządzeń, które będą rozdawane przez serwer VPN. Wykonawca wdroży odpowiedni przycisk i widok w interfejsie, który umożliwi wyżej wymienione czynności.

- Wykonawca zobligowany jest do udokumentowania wprowadzonych zmian w dokumentacji powykonawczej. Wykonawca zobligowany jest do przeprowadzenia sprawdzenia tabel w bazie danych MySQL, poddanie ich procesowi optymalizacji i usunięciu nadmiarów danych.

**Ad. 3. W ramach udzielonej gwarancji na wykonane prace programistyczne wskazane w punkcie 1 i 2 OPZ, Wykonawca udzieli bezpłatnego wsparcia serwisowego w ilości 50 godzin w zakresie:**

**1) administrowania Web API SAOL MUW w środowisku testowym
 i produkcyjnym;**

**2) oprogramowania serwera VPN w środowisku produkcyjnym;**

**3) integracji z systemami podległymi Zamawiającego;**

**4) udzielania konsultacji przedstawicielom Zamawiającego.**

Wykonawca udziela Zamawiającemu gwarancji na wykonane prace programistyczne na okres
12 miesięcy od daty podpisania przez obie Strony Protokołu Odbioru Końcowego bez uwag lub zastrzeżeń.

Wykonawca zobowiązany jest w ramach gwarancji do usuwania Błędów w funkcjonowaniu środowiska produkcyjnego, w czasie do 24h od momentu zgłoszenia Błędu przez Zamawiającego w terminach i środkami komunikacji określonymi poniżej.

Błąd – oznacza wystąpienie problemu polegającego na co najmniej jednym z poniższych:

a) występują istotne ograniczenia w działaniu komponentów Systemu wytworzonych przez Wykonawcę (ale nie powodujące jego przeciążenia);

b) nastąpiła awaria powodująca ograniczenie wydajności Systemu lub jego komponentów wytworzonych przez Wykonawcę.

Wykonawca jest zobowiązany do przyjmowania zgłoszeń Błędów w Dni Robocze. Wykonawca będzie przyjmował zgłoszenia dotyczące Błędów za pośrednictwem poczty elektronicznej wskazanej
w umowie z Wykonawcą.

W zgłoszeniu, o którym mowa powyżej Zamawiający określi kategorię Błędu. Wykonawca nie może zmienić kategorii Błędu bez pisemnej zgody Zamawiającego.

Wykonawca zobowiązuje się do świadczenia usług w ramach i w okresie udzielonej gwarancji na wykonane prace programistyczne tj. do udzielenia bezpłatnego wsparcia serwisowego w ilości 50 godzin w zakresie:

* 1. administrowania Web API SAOL MUW w środowisku testowym i produkcyjnym
	w terminie ustalonym przez Zamawiającego;
	2. oprogramowania serwera VPN w środowisku produkcyjnym w terminie ustalonym przez Zamawiającego;
	3. integracji z systemami podległymi Zamawiającego tj. nowo budowanymi systemami alarmowania i ostrzegania (powiatowymi i gminnymi) na terenie Województwa Mazowieckiego w terminie ustalonym przez Zamawiającego. Wykonawca w ramach tego wsparcia zapewni w szczególności:

a) możliwość wyjaśniania wątpliwości związanych z działaniem Systemu oraz zgłaszania nieprawidłowości w jego działaniu drogą telefoniczną, za pośrednictwem poczty elektronicznej;

b) w uzasadnionych przypadkach możliwość konsultacji oraz pomocy przy wyjaśnianiu wątpliwości oraz usuwaniu problemów związanych z działaniem Systemu;

c) dostęp do uaktualnień i poprawek oprogramowania udostępnianych przez producenta;

d) każdorazowe wsparcie serwisowe Wykonawcy zostanie potwierdzone poprzez sporządzenie stosownej notatki z realizacji zadania przesłanej drogą elektroniczną przez Wykonawcę do akceptacji Zamawiającego.

* 1. udzielania konsultacji przedstawicielom Zamawiającego w godzinach 8:00—16:00
	w Dni Robocze, e – mailem na adresy:

a) Jakub Sotowski, e-mail: jsotowski@mazowieckie.pl;

b) Krzysztof Janicki, e-mail: kjanicki@mazowieckie.pl;

c) Dawid Janicki, e-mail: djanicki@mazowieckie.pl;

d) Jacek Dudek, e-mail: jdudek@mazowieckie.pl.

Wykonawca zobowiązuje się do wykonywania obowiązków wynikających z gwarancji i wsparcia serwisowego w sposób zapobiegający utracie danych Zamawiającego, do których będzie miał dostęp w trakcie wykonywania naprawy. W przypadku, gdy dokonanie usunięcia wady wiąże się z ryzykiem utraty danych, Wykonawca zobowiązany jest poinformować o tym Zamawiającego przed przystąpieniem do usuwania wady oraz umożliwić Zamawiającemu dokonanie kopii zapasowych danych. Wykonawca zobowiązuje się do zapewnienia ciągłości wsparcia serwisowego w wypadku zakończenia działalności swojego przedsiębiorstwa w czasie, na który została udzielona gwarancja.