**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Oprogramowania SZK JAŚMIN –System Zarządzania Kryzysowego**

## Program SZK JAŚMIN - System Zarządzania Kryzysowego

Wykożystywany przez służby i instytucje państwowe:

**RAZEM** Ilość oprogramowania: 10 szt.

w tym:

Ilość licencji **klienckich**: 10 szt.,

Ilość licencji **serwerowych**: 2 szt.

Zamawiający dopuszcza systemy równoważne w zakresie wszystkich funkcji:

Program do zarządzania kryzysowego. Oferowany program w języku angielskim lub polskim musi umożliwiać kompleksowe **teleinformatyczne wsparcie**działań**administracji publiczneji   
i samorządowej podczas sytuacji ratowniczych i/lub kryzysowych oraz związanych z realizacją zadań prewencyjnych. System ten powinien wspierać procesy zarządzania,   
planowania, dowodzenia, kierowania,** a także **monitorowania** (obrazowania) rzeczywistych **zagrożeń o charakterze polityczno-militarnym oraz niemilitarnym.** Tworzenie powinno odbywać się na dowolnym komputerze lub urządzeniu przenośnym podłączonym do sieci, a sytuacje naniesione do programu powinny zostać automatycznie przesłane na inne stanowiska zarządzania. Opisywany program powinien być wykorzystywany przez inne komórki organizacyje służb publicznych (m.in.: Policji, Straży Pożarnej, Straży Granicznej, Ratownictwa Medycznego, Centrów Zarządzania Kryzysowego wszystkich szczebli oraz pozostałych struktur działających w czasie sytuacji kryzysowych), **a także resortu Obrony Narodowej**(np.: Sztabu Kryzysowego, Centrów i Zespołów Zarządzania Kryzysowego oraz Wojskowych Zgrupowań Zadaniowych). **Systemem powinien składać się ze specjalistycznego oprogramowania**/ Wielośrodowiskowego Zautomatyzowanego Systemu Zarządzania Kryzysowego -  (głównego komponentu omawianego rozwiązania) oraz dedykowanego sprzętu IT, **umożliwiającego globalne zarządzanie kryzysowe**- w tym monitorowanie stanu sił i środków wydzielonych do reagowania kryzysowego - np. **na terenie całego kraju. System ten powinien współpracować z pozostałymi Asystemami kompomentami programowymi wykorzystywanym w siłach zbrojnych RP** (w zależności od potrzeb powinien też np. wykorzystać wybrane ich funkcjonalności) oraz posiadać system bezpiecznej wymiany informacji (SBWI), który jest **eksploatowany w strukturach rządowych,** jednostkach i instytucjach im podległych, **w tym w MON**, gdzie funkcjonuje pod skróconą nazwą [SARON](https://www.teldat.com.pl/oferta/produkty/systemy/101-sbwi-saron.html)**i stanowi zasadniczą resortową platformę / sieć teleinformatyczną,** która**zapewnia**m.in**.: grupowe powiadamianie i alarmowanie, a także wymianę informacji**(w przypadku potrzeby **również niejawnych) pomiędzy dyżurnymi służbami operacyjnymi.**

**OPROGRAMOWANIE**

Główne funkcjonalności oprogramowania powinno zawierać:

* planowanie, wsparcie, kierowanie, koordynacja i kontrola działań, poprzez m.in.: mechanizmy optymalizacji rozwiązań (narzędzia kalkulacji, weryfikacji i symulacji), dynamiczne tworzenie zestawienia sił i środków, opracowywanie wariantów działań, plany zabezpieczenia logistycznego itp.;
* bieżące gromadzenie, przetwarzanie, agregacja i dystrybucja informacji o prowadzonych akcjach ratowniczych w zakresie:
  + **incydentów** (np.: zakłóceń bezpieczeństwa i porządku publicznego),
  + **zdarzeń** (np.: skażeń ujęć wody oraz pożarów lasów i/lub terenów przemysłowych),
  + **zagrożeń**(np.: epidemiologicznych, terrorystycznych lub związanych z procesami migracyjnymi oraz możliwością zawalenia mostów),
  + **informacji o terenie** (np.: obszarach zalewowych, stanie wałów przeciwpowodziowych oraz skażeniu chemicznym),
  + **danych o ludności** (np.: lokalizacji i ilości osób pozostających w budynkach lub obszarach działania, w celu dostarczenia im żywności lub ewakuacji),
  + **informacji o zasobach** (np.: ludzkich, obiektach, jednostkach, sprzęcie i środkach ochrony);
* automatyczne i bieżące raportowanie o stanie prowadzonych działań oraz dostępnych zasobach w zespołach ratowniczych;
* sprawne przekazywanie wybranym adresatom (strukturom, jednostkom oraz ich stanom osobowym, a także w razie potrzeby ludności) ważnych w danej chwili informacji (alarmów, różnego rodzaju powiadomień o zagrożeniach, poleceń, rozkazów, meldunków, raportów itp.) praktycznie w dowolne miejsce ich aktualnego usytuowania;
* współpraca z systemami innych resortów (w tym: Rządowego Centrum Bezpieczeństwa, Instytutu Meteorologii i Gospodarki Wodnej, Państwowej Straży Pożarnej, Policji, Straży Granicznej, Państwowego Ratownictwa Medycznego itp.) poprzez zastosowanie scentralizowanego portalu WWW - , umożliwiającego m.in. współdzielenie dokumentów i zautomatyzowaną dwukierunkową wymianę danych;
* zapewnić wysoki poziom bezpieczeństwa poprzez zapewnienie wieloklauzulowej wymiany i przetwarzania informacji (w tym również w sieciach niejawnych) poprzez zastosowanie odpowiednich mechanizmów: etykietowania, szyfrowania, uwierzytelniania i kontroli dostępu w sieciach teleinformatycznych (np.: zgodnych z koncepcją NATO XML Labelling, infrastruktury klucza publicznego PKI, VPN, IPSec i TLS/SSL);
* obrazowanie i monitorowanie na cyfrowych podkładach mapowych rzeczywistych sytuacji ratowniczych / kryzysowych na podstawie informacji GPS, danych wprowadzonych przez m.in. żołnierzy / funkcjonariuszy / ratowników oraz obrazów video i zdjęć z miejsca akcji;
* integracja i współpraca z bezzałogowymi statkami powietrznymi w zakresie bieżącej transmisji obrazu wideo z terenów / obszarów objętych blokadą, kwarantanną, akcjami poszukiwawczo-ratowniczymi, pożarami, powodziami itp.;
* modułowa architektura systemu zapewniająca dedykowane: oprogramowanie klienckie i serwerowe, funkcjonalności oraz usługi dla personelu lokalnego (realizującego proces zarządzania kryzysowego) i zdalnego (działającego w terenie), a także umożliwiająca elastyczną i łatwą rozbudowę o nowe możliwości oraz dodatkowe miejsca pracy;
* szeroka interoperacyjność systemu powinna gwarantować wymianę informacji z systemami resortu Obrony Narodowej, NATO i UE, dzięki zaimplementowanym standardom: MIP DEM B3.1, NFFI i FFI-MTF (STANAG 5527), Link 16 - JREAP-C (STANAG 5516 i STANAG 5518), VMF, NVG i JIPS, ADatP-3 (B11C/F, B12.2, B13.1 i B14) - STANAG 5510, JDSSEM (STANAG 4677), BRM (autorski i unikalny protokół replikacji danych na wąskopasmowych środkach łączności), HLA, DIS, SMTP, CBRN (ATP45), OTH-GOLD, WMS i WMF oraz APP-6(A)/(C);
* szeroki wachlarz usług sieciowych: rozmowy głosowe w technologii IP (VoIP), wideokonferencje (VTC), transmisje strumieniowe audio/wideo (RTMP), poczta elektroniczna (e-mail), portal WWW, rozmowy tekstowe (CHAT), FAX itp.;
* automatyczna i efektywna wymiana informacji poprzez dowolne środki radiowe (również w kanałach o niskiej przepustowości i wysokich zakłóceniach);
* wykorzystanie dostępnych mediów telekomunikacyjnych, np. sieci komórkowych GSM/LTE/CDMA i publicznych PSTN oraz VoIP;
* zarządzanie wszystkimi zasobami systemu (usługami, urządzeniami teleinformatycznymi i kontami użytkowników);
* zautomatyzowane mechanizmy i usługi replikacji oraz archiwizacji danych (wszystkich zdarzeń) w całym systemie;
* zdolność szybkiego i wygodnego dołączania służb ratowniczych i kryzysowych do systemu poprzez wykorzystanie aplikacji mobilnej zainstalowanej na współczesnych smartfonach, co umożliwia znaczące zautomatyzowanie procesu pozyskiwania informacji bezpośrednio od np. ratowników uczestniczących w akcji;
* monitorowanie osób przebywających na kwarantannie poprzez śledzenie ich miejsca pobytu;
* współpraca z systemami symulacyjnymi umożliwiająca: wielokrotne odtwarzanie wielu różnych wariantów działań, sytuacji, zachowań i efektów podejmowania decyzji oraz efektywną realizację szkoleń dla Użytkowników w zakresie m.in. skutecznego wykorzystania systemu oraz przygotowania się na eliminację i/lub minimalizację skutków praktycznie dowolnego zdarzenia kryzysowego.

Opracował: st. chor. Paweł MIKORSKI, tel. 261-658-235