

|  |  |
| --- | --- |
|  |  |

**Opis potrzeb i wymagań**

dla zadania

**Zaprojektowanie, budowa i wdrożenie Systemu Wczesnego Ostrzegania, Alarmowania
i Informowania 2.0 wraz ze sprzętową infrastrukturą serwerową oraz z usługą utrzymania przez okres 5 lat.**

**Uwaga 1:** Projekt, który jest przedmiotem niniejszego zamówienia jest projektem typu „Zaprojektuj i Wybuduj”. W „Opisie potrzeb i wymagań” znajdują się zatem ogólne wymagania Zamawiającego co do architektury systemu i jego funkcjonalności. Szczegóły implementacyjne zostaną uzgodnione z wybranym Wykonawcą na etapie tworzenia Projektu Techniczno-Wykonawczego Systemu.

**Uwaga 2:** Jeżeli w Opisie potrzeb i wymagań zostały wskazane znaki towarowe, patenty lub pochodzenie, Zamawiający w każdym przypadku dopuszcza rozwiązanie równoważne pod względem m.in. parametrów technicznych, materiałów, funkcji, zgodności (kompatybilności) itp. ze sprzętem lub oprogramowaniem wskazanym
przez Zamawiającego jako rozwiązanie referencyjne.

**Uwaga 3:** Sprzęt i wykorzystywane systemy operacyjne, oprogramowania oraz bazy danych nie mogą być przeznaczone przez producentów do wycofania z produkcji lub sprzedaży.

**SYSTEM OSTRZEGANIA ALARMOWANIA I INFORMOWANIA v. 2.0** musi składać się z:

1. **Aplikacji operacyjnej przeznaczonej do realizacji ostrzegania, alarmowania
i informowania, obsługi rzeczywistych zdarzeń i informacji, obsługi bazy danych sił i środków, komunikacji i administrowania zasobami i użytkownikami,**
2. **Aplikacji treningowej przeznaczonej do prowadzenia ćwiczeń i treningów**
3. **Aplikacji Testowej**
4. **Portalu Informacyjnego**
5. **Aplikacji OFFLINE instalowanej na komputerze użytkownika systemu**

Przeznaczeniem Systemu będzie:

* Gromadzenie danych o zagrożeniach z wykorzystaniem interfejsów API
z różnych dostępnych źródeł zewnętrznych.
* Gromadzenie i prezentacja informacji o zdarzeniach.
* Szybkie i skuteczne przekazywanie informacji podmiotom.
* Prezentacja zdarzeń i sytuacji kryzysowych na mapach cyfrowych.
* Gromadzenie, aktualizacja i prezentacja, w formie zestawień i na mapach cyfrowych, informacji o siłach i środkach dostępnych w miejscu wystąpienia zdarzenia lub sytuacji kryzysowej.
* Przekazywanie ostrzeżeń dla ludności, do Regionalnego Systemu Ostrzegania (RSO).
* Prognozowanie i wizualizacja zagrożeń, związanych z wystąpieniem, wypadków, katastrof lub awarii, z wykorzystaniem zaimplementowanych scenariuszy rozwoju sytuacji kryzysowych oraz danych historycznych.
* Prognozowanie skażeń powstałych w wyniku wystąpienia katastrof i awarii
w zakładach dużego i zwiększonego ryzyka wystąpienia poważnej awarii przemysłowej w oparciu o „Zasady postępowania ratowniczego” – pozwalający wizualizować na mapie i prognozować skażenia na podstawie aktualizowanych przez IMGW danych pogodowych.
* Tworzenie i przesyłanie meldunków w standardzie AdatP-3 do systemu **SI** PROMIEŃ oraz wizualizacja otrzymanych poprzez API meldunków prognozowanych stref skażeń z systemu SI PROMIEŃ.
* Gromadzenie, aktualizacja i prezentacja w formie tabelarycznej i na mapach cyfrowych informacji o wolnych łóżkach w szpitalach.
* Możliwość wprowadzania do systemu i wykorzystania, podczas wystąpienia sytuacji kryzysowej, procedur i scenariuszy wynikających z planu działania zarządzania kryzysowego.
* Generowanie i przekazywanie raportów i zestawień obrazujących zarówno aktualną sytuację jak i dane historyczne.
* Prowadzenie w sposób zautomatyzowany ćwiczeń i treningów z podmiotami systemu z wykorzystaniem aplikacji treningowej.
* Możliwość wykorzystania wersji offline systemu na wypadek braku dostępu
do Internetu. Synchronizacja wersji offline z wersją operacyjną po ponownym uzyskaniu dostępu do Internetu.
* Prezentacja informacji dla społeczeństwa na Portalu Informacyjnym.
* Globalny generator tworzenia formularzy raportów.

 W Systemie zarejestrowanych będzie ok. 45000 kont użytkowników, z tego dla pracy Online należy zapewnić dostęp do Systemu dla ok. 15000 użytkowników.

System musi posiadać komercyjną bazę danych obsługującą nieograniczoną ilość wątków
i posiadającą wsparcie 24/7 przez 365 dni w roku.

**WYKONAWCA, KTÓREMU ZOSTANIE UDZIELONE ZAMÓWIENIE, BĘDZIE MUSIAŁ WYKONAĆ NASTĘPUJĄCE ZADANIA:**

1. Przeprowadzenie niezbędnych uzgodnień z Zamawiającym, opracowanie Projektu Techniczno - Wykonawczego (PTW), oraz opracowanie Harmonogramu Realizacji Wdrożenia (HRW), z wyszczególnieniem „kamieni milowych” wdrożenia oraz dat
ich osiągnięcia. Zatwierdzenie PTW i HRW przez Zamawiającego będzie pozwalało na dalszą realizację zadania
2. Zakup sprzętu, oprogramowania, wymaganych licencji, gwarancji wraz z supportem na okres 5 (pięciu) lat
3. Wykupienie usługi dostawy internetu symetrycznego wraz z publiczną adresacją IP
do serwerowni we Wrocławiu i Poznaniu o przepustowości 10 Gb/s na okres 5 lat
4. Zakup i utrzymanie nazwy domeny wskazanej przez Zamawiającego
wraz z certyfikatem SSL typu Wildecard na okres 5 lat.
5. Montaż, uruchomienie, instalacja oraz konfiguracja sprzętu i oprogramowania
w lokalizacjach
6. Zbudowanie Aplikacji Operacyjnej, Treningowej, Testowej i OFFLINE
7. Wykonanie Portalu Informacyjnego
8. Przeprowadzenie testów akceptacyjnych całego Systemu na podstawie opracowanych przez Wykonawcę i zaakceptowanych przez Zamawiającego scenariuszy testów
9. Przeprowadzenie szkoleń dla Administratorów Systemu
10. Przeprowadzenie szkoleń dla Użytkowników Systemu
11. Opracowanie i dostarczenie dokumentacji powykonawczej Systemu
12. Opracowanie i dostarczenie wszystkich wymaganych instrukcji dla Administratorów i Użytkowników Systemu
13. Przeprowadzenie audytu bezpieczeństwa i uzyskanie akceptowalnego poziomu zabezpieczenia Systemu z audytu bezpieczeństwa, jaki Wykonawca zleci firmie specjalizującej się w Audytach Bezpieczeństwa. Zamawiający wskaże Wykonawcy wymagania i parametry wg których powinien być przeprowadzony Audyt Bezpieczeństwa
14. Przeprowadzenie i opracowanie analizy ryzyka Systemu. W opracowaniu muszą znajdować się opisy zasobów systemu teleinformatycznego, zagrożenia oddziaływujące na zasoby, podatności zasobów lub zabezpieczeń i skutki działania zagrożeń
15. Opracowanie planu ciągłości działania Systemu
16. Przekazanie Zamawiającemu kodów źródłowych do wytworzonych aplikacji: operacyjnej, treningowej, testowej, Portalu Informacyjnego oraz Aplikacji OFFLINE, które z chwilą ich odbioru stają się wyłączną własnością Zamawiającego.Zamawiający posiada wyłączne autorskie prawa majątkowe do Systemu
17. Udzielenie bezterminowej, nielimitowanej licencji na dostarczone(wykonane)
w ramach realizacji projektu oprogramowanie Systemu
18. Przekazanie Zamawiającemu wszystkich wykorzystywanych w projekcie licencji
19. Przekazanie Zamawiającemu potwierdzenia zakupu gwarancji producenta
wraz ze wsparciem na okres 5 (pięciu) lat
20. Nieodpłatne świadczenie usługi utrzymania całego Systemu przez okres 5 (pięciu) lat od daty podpisania Protokołu Końcowego Odbioru Prac

**Szczegółowy opis poszczególnych zadań podany jest w kolejnych rozdziałach Opisu potrzeb i wymagań**

**AD. 1 Aplikacja Operacyjna**

1. **Wymagania ogólne:**
* Aplikacja musi być zaprojektowana w formie portalu internetowego
* Aplikacja musi być aplikacją jednorodną, posiadającą jednolity interfejs użytkownika. Dotyczy to także wykonania aplikacji w postaci kilku niezależnych komponentów. Wykonawca musi zapewnić w takim przypadku:
1. jednolity interfejs użytkownika (GUI) we wszystkich komponentach;
2. jednolity system pomocy i sygnalizacji błędów;
3. jednokrotne logowania się do systemu – zaimplementowane SSO (*Single Sign On*). Niezależnie, do którego komponentu zalogujemy się najpierw
w danej sesji, będzie to jedyne logowanie w tej sesji;
4. administrowanie całą aplikacją, a nie poszczególnymi komponentami;
5. jedno miejsce sterowania uprawnieniami do wszystkich komponentów.
* Aplikacja musi być responsywną, tzn. graficznie dostosowaną do rozmiaru wyświetlacza, na którym jest prezentowana;
1. **Główne funkcjonalności systemu**

**Moduł komunikacyjny:**

* Wyślij wiadomość (musi umożliwiać nadawcy zarówno wysłanie informacji
jak i śledzenie przez nadawcę postępu w zapoznawaniu się z jej treścią
przez adresatów. Funkcjonalność musi umożliwiać wygenerowanie w postaci pliku EXCEL lub PDF wykazu wysłanych, doręczonych i niedoręczonych informacji)
* Grupy kontaktów (ta funkcja musi umożliwiać proste tworzenie grup kontaktów
przez każdego użytkownika dla jego potrzeb poprzez wybieranie instytucji. Administrator generalny powinien mieć możliwość tworzenia grup do wykorzystania przez użytkowników szczebla wojewódzkiego i centralnego (tzw. grupy globalne
np. PCZK województwo dolnośląskie, PCZK województwo wielkopolskie, WCZK-Kraj itp., służby inspekcje i straże województwo dolnośląskie, służby inspekcje
i straże województwo wielkopolskie, służby inspekcje i straże - kraj,
* Odbiorcy (musi umożliwiać definiowanie instytucji (osób funkcyjnych)
z jej podstawowymi parametrami jak: nazwa, adres, tel. fax, e-mail, stanowisko)
* Książka Globalna (odzwierciedlająca strukturę hierarchiczną administracji umożliwia wyszukiwanie instytucji, osób, edycję ich danych):
	+ - Krajowy
		- Wojewódzki
		- Powiatowy
		- Gminny
* Alert RCB (funkcja musi umożliwiać w przygotowanym predefiniowanym formularzu sformułowanie wniosku do Dyrektora RCB o uruchomienie Alertu RCB
na określonym obszarze: powiatu (powiatów), województwa
	+ Wyślij
	+ Archiwum wysłanych wniosków
* Skrzynka odbiorcza
	+ Wiadomości
	+ Nowe wiadomości
	+ Ostrzeżenia
	+ Nowe ostrzeżenia
	+ Alarmy
	+ Nowe alarmy
* Wysłane wiadomości
* Kontakty (wyświetla dla użytkownika wyłącznie kontakty do szczebla wojewódzkiego włącznie)
* Mój profil (wyświetla dane profilu użytkownika umożliwiając ich aktualizację
w zakresie telefonów, fax, e-mail)
* Komunikaty systemowe (umożliwia śledzenie każdemu użytkownikowi stanu powiadamiania instytucji o wprowadzonym do systemu zdarzeniu)
* Władze (możliwość wprowadzenia informacji dotyczącej kierowniczej kadry poszczególnych szczebli administracji, służb inspekcji i straży. Szczebel krajowy jest widoczny wyłącznie dla podmiotów szczebla krajowego i WCZK)
	+ Szczebel Krajowy
	+ Szczebel Wojewódzki
	+ Szczebel Powiatowy
	+ Szczebel Gminny
	+ Sołectwa (sołtys)
* FAX
	+ Wyślij fax (jeśli województwo posiada usługę webową umożliwiającą wysyłanie FAX. Funkcja dodawania, edytowania i kasowania serwera faxów powinna być możliwa z poziomu administratora np. Wojewódzkiego)
	+ Archiwum wysłanych FAX
* Email
	+ Wyślij email (system musi umożliwiać **wyłącznie wysyłanie e-mail,**
	do systemu ze względów bezpieczeństwa nie będą wpływać żadne e-mail)
	+ Archiwum wysłanych e-mail
* SMS (wyłącznie dla województw, które mają systemy masowej wysyłki SMS posiadające API na które można wysyłać zlecenia wysyłki. Funkcja dodawania, edytowania i kasowania bramki SMS powinna być możliwa z poziomu administratora np. Wojewódzkiego)
	+ Wyślij SMS (jeśli województwo posiada aplikację posiadającą API umożliwiającą integrację i masową wysyłkę SMS). Dla województw
	nie posiadających takich systemów ta funkcjonalność nie będzie włączona.
	+ Archiwum wysłanych SMS

**Moduł  operacyjny**

Musi realizować ostrzeganie, alarmowanie i informowanie o zagrożeniach spowodowanych działaniami człowieka. Każde wprowadzone zdarzenie geolokalizuje miejsce i jest wizualizowane na mapach cyfrowych (BDOT, ortofotomapa, OpenStreetMap);

**Główne funkcjonalności modułu operacyjnego:**

* Dodaj zdarzenie
* Dodaj zdarzenie ZDR
* Dodaj zdarzenie bez alarmu (np. zdarzenie historyczne nie bieżące które nie wymaga natychmiastowego ostrzegania – tylko dokumentuje jego wystąpienie)
* Wyślij ostrzeżenie , alarm (po wysłaniu informacji o tym statusie u użytkowników ostrzeganych instytucji musi być emitowany dźwięk ostrzeżenia oraz musi pulsować ikona alarmu (ostrzeżenia w górnej części paska aplikacji)
* Dodaj meldunek MGCO (meldunek jak Międzynarodowa Centrala Ostrzegawczo – Alarmowa dla Odry). Funkcjonalność dostępna wyłącznie dla województw:
	+ Dolnośląskiego
	+ Opolskiego
	+ Śląskiego
	+ Lubuskiego
	+ Zachodniopomorskiego
	+ MKOO Wrocław (Międzynarodowa Komisja Ochrony Odry
	przed zanieczyszczeniami). Wysyłany meldunek będzie wg jednolitego wzoru – zgodnie ze schematem alarmowania zawartym w „Planie Ostrzegawczo
	– Alarmowym dla Odry”.

W odniesieniu do działania MGCO państwa członkowskie Czechy i Niemcy otrzymują meldunek wygenerowany z systemu w postaci e-mail i FAX.

* Dodaj meldunek SI PROMIEŃ (meldunek wg metodyki ATP-45D w standardzie ADATP3). Wysyłka do CD KSWSiA. Meldunek z CD KSWSiA wraca do systemu
w postaci prognozy. Prognoza wchodzi do systemu poprzez moduł komunikacyjny
i podlega przekazaniu – zgodnie ze schematem informowania ostrzegania
– jak w odniesieniu do zdarzeń. (UWAGA – schemat zgodny z Krajowym Planem Współdziałania).
	+ Wszystkie zdarzenia (Wyświetla wszystkie zdarzenia bieżące. Posiada ikonki („RSO”, „PI” „**Przekaż do RCB”,** z wykorzystaniem których użytkownik (dyżurny WCZK) publikuje informację w tych serwisach oraz przekazuje informację do szczebla krajowego RCB)
* Archiwum zdarzeń (umożliwia wyświetlenie wyłącznie na komputerze lokalnym zdarzeń historycznych zamkniętych)
* Kategoria rodzaj zdarzenia (Na szczeblu krajowym obowiązuje katalog zagrożeń zgodny z KPZK, na szczeblu wojewódzkim i w województwie obowiązuje katalog zgodny z WPZK danego województwa. System musi umożliwiać automatyczne powiązanie zagrożeń wynikających z katalogów WPZK z KPZK)
* Procedury (system musi umożliwiać każdemu użytkownikowi wprowadzenie swoich procedur wynikających z planu zarządzania kryzysowego, które wyświetlają się
w chwili wprowadzenia zdarzenia i wymagają potwierdzenia ich realizacji umożliwiając pominięcie kroku procedury po wpisaniu uzasadnienia pominięcia tego kroku. System musi umożliwiać powrót do realizacji pominiętego kroku procedury.)
	+ Procedury postępowania
	+ Edycja procedury postępowania
	+ Przypisanie procedury do zagrożenia
	+ Procedury użytkownika
* Zgłaszający zdarzenie (instytucja, imię i nazwisko wprowadzającego)
* raport z dyżuru (możliwość zdefiniowania dyżurów 8 godz., 12 godz. i 24 godz. pełnionych jednoosobowo, dwuosobowo, trzyosobowo i czteroosobowo)
	+ szczebel gminny
	+ szczebel powiatowy
	+ szczebel wojewódzki
	+ szczebel krajowy (RCB, CZK Ministerstw)
* sytuacja kryzysowa (możliwość przekazania zarządzania zdarzeniem)
* informacje z IMGW (wszystkie informacje które do systemu przekazuje IMGW
w standardzie XML)
	+ Ostrzeżenia meteorologiczne (zbiorcze i powiaty) /opis i grafika/
	+ Ostrzeżenia hydrologiczne /opis i grafika/
	+ Odwołania ostrzeżeń – wszystkie /opis i grafika/
	+ Prognozy pogody
		- Krótkoterminowe
		- Średnioterminowe
		- Biuletyn 5- dniowy
	+ Prognozy zjawisk niebezpiecznych
	+ Komunikaty meteorologiczne
	+ Prognozy stanów wody /dla podstawowych profili osłony hydrologicznej/
	+ Średni opad zlewni
	+ Stan zbiorników
	+ Prognoza wezbrania powodziowego /opis i grafika/
	+ Sytuacja radarowa z hydromonitora
	+ Wodowskazy - z hydromonitora
	+ Wizualizacja siły i kierunku wiatru
* Utrudnienia drogowe (Przekazywane do systemu w standardzie XML z możliwością geolokalizowania ich na mapie cyfrowej włączane i wyłączane na żądanie
jako warstwa).
* Informacja z RZGW Wody Polskie (dotycząca stanu rzek, stanu urządzeń wodnych)
* System SI Promień (funkcjonalność musi umożliwiać utworzenie meldunku
w standardzie AdatP3 i wysłanie go do API systemu CD KSWSiA, wczytania meldunku prognozy otrzymanej poprzez API z CD KSWSiA.
	+ Meldunek „do systemu” SI Promień
	+ Meldunek „z systemu” SI Promień
* Informacja z systemu ruchu pociągów (lokalizacja pociągu na mapie, rodzaj składu pasażerski/towarowy, nr pociągu)

 Informacja o zdarzeniu wg zadanego klucza automatycznie po jej wprowadzeniu musi być dostarczana w czasie **do 5 minut** do odbiorcy docelowego.

Odbiorcami docelowymi są:

* + - wszyscy użytkownicy szczebla gminnego na terenie którego doszło do zdarzenia oraz gmin sąsiadujących danego województwa;
		- wszyscy użytkownicy szczebla powiatowego na obszarze którego wprowadzono zdarzenie;
		- wszyscy użytkownicy służb inspekcji i straży szczebla wojewódzkiego na terenie którego doszło do zdarzenia;
		- jeśli do zdarzenia doszło na terenie gminy sąsiadującej z obszarem innego województwa – odbiorcą jest także WCZK województwa sąsiadującego.
		- **Użytkownicy szczebla centralnego (krajowego) otrzymują informację
		po zaznaczeniu jej przez dyżurnego WCZK jako „przekaż do RCB”. Zaznaczona w ten sposób informacja o zdarzeniu Dyżurnemu RCB sygnalizuje się w ten sam sposób jak dla przyjętej automatycznej procedury (dźwiękowo i wizualnie).**

 Ponadto, użytkownik WCZK UW powinien mieć możliwość uzupełnienia informacji
o zdarzeniu do WCZK innego województwa oraz do szczebla centralnego (RCB, Ministerstw).

Użytkownik który wprowadził zdarzenie, i szczeble nadrzędne muszą posiadać możliwość uzupełniania informacji o zdarzeniu, podejmowanych działaniach, zaangażowanych siłach
i środkach. System musi automatycznie informować o uzupełnieniu (dopisaniu) informacji dotyczącej wprowadzonego zdarzenia – zgodnie z kluczem informowania.

Każde zdarzenie musi zawierać min. następujące dane:

* zgłaszający (imię, nazwisko, instytucja zgłaszająca)
* Data i godzina zdarzenia
* Priorytet (Wysoki, Normalny, Niski)
* Rodzaj (bieżące, archiwalne)
* Kategorię zdarzenia – zgodną z katalogiem obowiązującym na obszarze danego województwa i wynikającą z Wojewódzkiego Planu Zarządzania Kryzysowego
* Rodzaj zdarzenia – zgodnie z WPZK
* Procedurę działania (dla każdego szczebla: gmina, powiat, województwo, RCB)
– wynikającą z planów zarządzania kryzysowego dla danego szczebla
* Charakter (krajowy, wojewódzki, powiatowy, gminny)
* Czynność (przyjęcie zgłoszenia, przekazanie zgłoszenia)
* Wybór lokalizacji zagrożenia umożliwiający pozycjonowanie zdarzenia na mapie:
* poprzez wskazanie na mapie,
* po danych adresowych (kraj, województwo, powiat, gmina, miejscowość, ulica, nr domu)
* współrzędne GPS
* Liczba osób poszkodowanych ogółem
	+ w tym dzieci
* Liczba ofiar śmiertelnych
	+ w tym dzieci
* Miejsce zdarzenia
* Opis zdarzenia
* Uwagi

**Zdarzenie (informacja) wprowadzona na obszarze innego kraju nie generuje alarmów – tylko informuje szczebel centralny RCB).**

RCB (inny szczebel centralny) musi mieć możliwość dalszego przekazania informacji
na szczebel wojewódzki.

Każda kategoria zdarzenia szczebla wojewódzkiego musi być powiązana z kategorią ujętą
w Krajowym Planie Zarządzania Kryzysowego.

Każde zdarzenie musi posiadać następujące cechy podczas wprowadzania:

* Generować po dostarczeniu do użytkownika sygnał akustyczny oraz wizualny wyświetlanego obiektu w postaci czerwonego dzwonka. Kliknięcie
na dzwonek powoduje wyświetlenie pełnej informacji o wprowadzonym zdarzeniu z możliwością wyświetlenia geolokalizacji zdarzenia i pełnej informacji o zdarzeniu.
* Po kliknięciu na mapie w ikonkę symbolu musi się wyświetlić opis zdarzenia, informacje o osobach poszkodowanych, nazwa województwa, powiatu i gminy
* Każde zdarzenie musi posiadać opcje śledzenia informacji o jego przeczytaniu. Z każdego wprowadzonego zdarzenia musi być generowany raport dotyczący do kogo wysłano informację o zdarzeniu, kto ją odebrał z podziałem
na szczeble i jednostki organizacyjne (gmina, powiat, województwo, szczebel centralny)
* Dla każdej informacji o zdarzeniu musi istnieć możliwość wysłania
jej do publikacji w RSO, Portalu informacyjnym w zakładce danego województwa. Uprawnienie wyłącznie szczebla wojewódzkiego (WCZK). Każda informacja przekazywana do publikacji (RSO lub PI) podlega edycji przed przekazaniem do publikowania.
* Każde zdarzenie może zostać przeniesione do archiwum przez WCZK właściwe dla danego województwa oraz RCB. Musi istnieć możliwość przywrócenia w tryb ponownego wyświetlania z pozycjonowaniem zdarzenia na mapie.
* Każde zdarzenie wprowadzone do systemu przechowywane jest w module operacyjnym, w którym muszą być następujące zakładki z funkcjonalnościami:
	+ - Dodaj zdarzenie
		- Dodaj zdarzenie ZDR, ZZR (zakładu dużego ryzyka wystąpienia poważnej awarii przemysłowej, zakładu zwiększonego ryzyka wystąpienia poważnej awarii przemysłowe)
		- Wyślij ostrzeżenie /alarm
		- Moje zdarzenia (zdarzenia wprowadzone przez użytkownika)
		- Wszystkie zdarzenia (wszystkie zdarzenia dla określonego szczebla administracji gmina, powiat, województwo)
		- Archiwum zdarzeń (katalog w którym przechowywane są wszystkie informacje o zdarzeniach przeniesionych do archiwum)
		- Informacja o kategoriach (rodzajach zdarzeń – zgodnie z WPZK
		z możliwością edycji na szczeblu RCB, administratora generalnego systemu
		- Edycja procedur działania zgodnie z planami zarządzania kryzysowego (dla każdego szczebla administracji: gmina, powiat, województwo, krajowy)
		- Przypisanie procedury do rodzaju zagrożenia na każdym szczeblu: gmina, powiat, województwo, krajowy
		- Zgłaszający zdarzenie (możliwość zdefiniowania podmiotów zgłaszających zdarzenie np. GCZK, nazwa gminy, PCZK, WCZK, RCB itd. z możliwością edycji, dodawania nowych pozycji
		i ich usuwania.
		- Procedury użytkowników (centralne miejsce w którym znajduje się zbiorcza informacja o wprowadzonych przez użytkowników procedurach z podziałem na szczebel krajowy, województwa, powiaty
		i gminy (imię i nazwisko wprowadzającego procedurę, nazwa instytucji, sygnatura procedury, nazwa. Użytkownik danego szczebla widzi tylko swoje procedury. Administrator generalny, **RCB widzi wszystkie procedury z powyższym podziałem administracyjnym;**
* Każda informacja wprowadzana do systemu jako zdarzenie przychodzi
jako AWIZO w module komunikacyjnym, który jest miejscem przechowywania wszystkich informacji z podziałem na zdarzenia, ostrzeżenia, alarmy, informacje itd.

• geolokalizowanie wypadków, katastrof i awarii spowodowanych działaniami człowieka na mapach cyfrowych, w tym zagrożeń obszarowych;

• system będzie umożliwiał publikowanie informacji o wszystkich zdarzeniach spowodowanych działaniami człowieka na stronach internetowych oraz ich przekazywanie do publikacji w RSO (Regionalnym Systemu Ostrzegania);

• tworzenie doraźnych zestawień informacji za dowolny okres z wprowadzonych
do systemu zdarzeń informacji;

• zaimplementowane obowiązujące „Zasady postępowania ratowniczego” na podstawie ERG 2020 umożliwi prognozowanie obszarów ostrzegania i ewakuacji w razie wystąpienia katastrof i awarii spowodowanych działaniami człowieka w zakładach dużego i zwiększonego ryzyka wystąpienia poważnej awarii przemysłowej spowodowanych przez człowieka w oparciu o „Zasady postępowania ratowniczego”. System umożliwi wizualizowanie i prognozowanie na mapie obszaru skażenia wykorzystując aktualizowane przez IMGW dane pogodowe;

• możliwość administrowania systemem w szczególności uprawnieniami użytkowników, tworzeniem nowych szablonów raportowania;

• na wypadek wystąpienia poważnych zdarzeń, awarii i katastrof system będzie posiadał możliwość gromadzenia i wyświetlania informacji dotyczących potencjalnie dostępnej bazy łóżkowej dla rozlokowania osób poszkodowanych;

• aplikacja operacyjna będzie służyć do rzeczywistego obiegu informacji a aplikacja treningowa do doskonalenia oraz ćwiczeń;

• system będzie posiadał dane zasobów możliwych do wykorzystania na wypadek wystąpienia ww. katastrof, awarii i innych nagłych zdarzeń;

• możliwości analityczno-statystyczne i modelowania np. wizualizację zagrożeń obszarowych związanych z wystąpieniem ww. wypadków, katastrof i awarii;

• poprzez okresowe zasilanie systemu danymi o ilości osób zameldowanych pod danym adresem (z systemu PESEL lub Źródło) system będzie umożliwiał w module analiz przestrzennych dokonywanie analizy ilości osób znajdujących się w strefach zagrożenia (niebezpiecznych);

• „przetwarzanie (otrzymywanie, gromadzenie, wysyłanie, wizualizowanie) informacji
na potrzeby zarządzania kryzysowego”.

• zdarzenia, zasoby muszą być wizualizowane symbolami na mapie cyfrowej – zgodnie
z Decyzją Ministra Spraw Wewnętrznych i Administracji z dnia 18 kwietnia 2008 r.
Dz. U. Nr 5.

**Baza Danych Sił i Środków** (musi posiadać niżej wyszczególnione funkcjonalności dostępne dla każdego użytkownika.

* Szukaj zasobów
* baza sił i środków
	+ Alarmowanie
	+ farmacja
	+ hotele
	+ hostele
	+ infrastruktura
	+ Łączność
	+ łodzie ratunkowe
	+ magazyn przeciwpowodziowy
	+ magazyny i chłodnie
	+ Maszyny i urządzenia
	+ materiały i środki zabezpieczenia ludności
	+ miejsca noclegowe
	+ noclegownie
	+ ogrzewalnie
	+ dworce kolejowe
	+ motoryzacyjne zakłady naprawcze
	+ narzędzia środki i materiały
	+ OSP
	+ Organizacje pozarządowe
	+ PK HNS
	+ pojazdy
	+ pojazdy zimowego utrzymania dróg
	+ pralnie
	+ produkcja zwierzęca
	+ Przychodnie POZ
	+ przyrządy pomiarowe
	+ ratownictwo medyczne
	+ ratownictwo specjalistyczne
	+ ratownictwo techniczne
	+ GOPR
	+ WOPR
	+ schroniska
	+ Składnice i rozlewnie paliw
	+ stacje paliw
	+ służby porządkowe
	+ Policja
	+ sprzęt chemiczny
	+ sprzęt ciężki
	+ sprzęt i materiały
	+ sprzęt kwatermistrzowski
	+ sprzęt łączności
	+ Statki powietrzne
	+ szpitale
	+ ZMSz
	+ środki ratownicze
	+ urządzenia
	+ Weterynaria
	+ zakłady DDD
	+ spalarnie odpadów
	+ zakłady produkujące żywność
	+ zakłady utylizacyjne
	+ żywienie zbiorowe
	+ mogilniki
	+ punkty poboru opłat
	+ dworce autobusowe
	+ lotniska
	+ lądowiska
	+ Lotnicze Pogotowie Ratunkowe

System musi zapewnić funkcjonowanie aplikacji OFFLINE, którą użytkownik instaluje
na wybranym stanowisku pracy. Dostęp do zasobów OFFLINE jest dostępny na podstawie loginu i hasła zdefiniowanego dla użytkownika systemu nadanego przez administratora szczebla wojewódzkiego. Konto OFFLINE będzie takie samo jak zdefiniowane dla Aplikacji Operacyjnej. Dostęp do OFFLINE przydziela administrator generalny i będzie on dostępny wyłącznie dla użytkownika, który zainstalował aplikację OFFLINE.

Zapytanie wysłane do systemu dotyczące zasobu musi wyświetlić jego lokalizację na mapie cyfrowej np.:

* Zapytanie o zasób w gminie (gminach) musi wyświetlić w zestawieniu oraz na mapie zasoby gminne (wybranych gmin).
* Zapytanie o zasób na obszarze powiatu (powiatów) musi wyświetlić w zestawieniu oraz na mapie zasoby wybranego powiatu (powiatów).
* Zapytanie o zasób w województwie (województwach) musi wyświetlić w zestawieniu oraz na mapie zasoby tych wybranych województw.

Po kliknięciu w symbol zasobu na mapie musi się wyświetlać informacja o zasobie (nazwa, ilość, właściciel, dane adresowe i kontaktowe).

**Analizy przestrzenne –** system musi umożliwiać tworzenie, edycję, usuwanie i wyświetlanie analiz przestrzennych, które mogą być analizami użytkownika przypisanymi wyłącznie
dla użytkownika lub analizami widocznymi dla użytkowników systemu – zgodnie z podziałem administracyjnym. System musi umożliwiać jednoczesne wyświetlanie wszystkich zaznaczonych do wyświetlenia analiz jednocześnie. System musi umożliwiać użytkownikowi, który opracował analizę blokadę edycji analizy.

Moduł musi umożliwiać wyświetlenie analizy z podziałem administracyjnym:

* Krajowe widoczne dla użytkowników szczebla centralnego, wojewódzkiego
lub dla wszystkich użytkowników systemu)
* Wojewódzkie widoczne wyłącznie dla użytkowników danego województwa)
i szczebla centralnego lub innych wybranych szczebli
* Powiatowe widoczne wyłącznie dla użytkowników szczebla gminnego, powiatowego, wojewódzkiego i szczebla centralnego
* Gminne widoczne wyłącznie dla użytkowników danego województwa szczebla gminnego, powiatowego, wojewódzkiego i szczebla centralnego

**Rodzaj analiz**

* katastrofa drogowa
* katastrofa kolejowa
* katastrofa lotnicza
* Skażenie chemiczne
* zagrożenie weterynaryjne
* zagrożenie powodziowe
* zagrożenie pożarowe
* zagrożenie terrorystyczne
* brak wody
* susza
* analiza SI Promień
* modułu chemicznego
* cyberbezpieczeństwo (na podstawie zdarzeń bieżących lub archiwalnych
* inne

typ analiz:

* Okrąg
	+ po wstępnych predefiniowanych parametrach np. 3 i 10 kilometrów
	+ po parametrach wybieranych przez użytkownika
* prostokąt
* trójkąt
* linia
* punkt
* dowolny kształt do obrysowania (np. z użyciem ekranu dotykowego lub myszy
w postaci pióra)
* dowolny kształt obrysowania odcinkami
* metoda wybrania obszaru predefiniowanego (kodem teryt)
	+ kraj
	+ województwo
	+ powiat
	+ gmina
	+ miejscowość

**Moduł obsługi mapy**

* Zmień serwis mapowy
	+ BDOT
	+ Ortofotomapa
	+ OpenStreetMap (Polska i świat)
* Skalowanie mapy min. 20 poziomów od 1:2000
* Mapy muszą mieć odzwierciedlenie w następujących układach współrzędnych:
	+ Geograficzne
		- WGS-84
		- PUWG92
		- PUWG2000
	+ UTM
* Odblokuj mapę (na drugi monitor)
* Zablokuj mapę (do obsługi na jednym monitorze)
* Eksportuj bieżącą mapę widok ekranu (czystą lub z analizami i wybranymi obiektami zasobów, zdarzeń) (xls, xlsx, PDF, jpg, RTF)
* Serwis WMS (WMTS)
	+ Mapa ryzyka powodziowego
	+ Mapa zagrożenia powodziowego
	+ Dołącz serwis WMS (WMTS) z geoportalu lub innego adresu.
	+ Włączanie predefiniowanych warstw GIS (system musi umożliwiać nieograniczoną możliwość jednoczesnego włączania przygotowanych
	w systemie warstw GIS)
	+ Wyłączanie warstw wyświetlanych (System musi umożliwiać wyłączanie każdej wyświetlonej na mapie warstwy tematycznej GIS)

Uwaga: Mapa po zalogowaniu jest czysta bez zasobów, ale z lokalizacją miejsc obowiązujących zdarzeń.

 **Zarządzanie publikacją informacji na zewnątrz systemu**

* Przekaż do RSO
* Archiwum informacji (zdarzeń) przekazanych do RSO
* Przekaż do PI (Portalu Informacyjnego) na stronę www odpowiednią dla danego województwa
* Archiwum informacji (zdarzeń) przekazanych do PI
* Informacja o opublikowanych komunikatach ostrzeżeniach alarmach alertach

**Moduł Raportowania**

* **Raport z dyżuru** (dla podmiotów pełniących dyżury)
	+ szczebel gminny
	+ szczebel powiatowy
	+ szczebel wojewódzki
	+ szczebel centralny
* **raport doraźny**
	+ szczebel gminny
	+ szczebel powiatowy
	+ szczebel wojewódzki
	+ szczebel centralny
* **raport dobowy**
	+ szczebel gminny
	+ szczebel powiatowy
	+ szczebel wojewódzki
	+ szczebel centralny
* **raport sytuacyjny –** wg zadanego formatu raportowania
	+ szczebel gminny
	+ szczebel powiatowy
	+ szczebel wojewódzki
	+ szczebel centralny
* raport ze zdarzenia generowany automatycznie po wprowadzeniu zdarzenia
do systemu. Zawiera informacje wprowadzone w związku z wystąpieniem zdarzenia (zagrożenia): współrzędne zdarzenia, podmiot wprowadzający, informowane podmioty oraz skuteczność dostarczenia (odebrania) informacji przez każdego alarmowanego użytkownika.
* Generowanie raportu zdarzeń dla określonego zakresu czasowego
* wykres ilości zdarzeń według kategorii
* wykres ilości osób poszkodowanych wg kategorii
* inne raporty wytworzone przez generator formularzy raportowania

Dla wszystkich raportów musi być zdefiniowana możliwość wyeksportowania do najbardziej popularnych formatów: (doc, rtf, xls, PDF, JPG)

**Moduł  obsługi zdarzeń chemicznych – zgodny z Zasadami postępowania ratowniczego ERG**

* Zaznacz punkt skażenia
* archiwum analiz chemicznych
* analiza obszaru skażenia

**Generator formularzy raportowania**

Moduł ten odpowiada za scentralizowane tworzenie nowych formularzy raportowania przez:

* wybrane podmioty i szczeble raportujące
* scentralizowane raportowanie hierarchiczne np:
	+ gmina
	+ powiat
	+ województwo
	+ kraj

lub np.

* Szpitale szczebel powiatu
* Szpitale szczebel wojewódzki
* Szpitale resortowe
* Inne szpitale
* Szpitale województwo
* Szpitale kraj

Utworzony formularz musi  umożliwiać automatyczne sumowanie danych w tabeli
na każdym szczeblu np.

* + gmina
	+ powiat
	+ województwo
	+ kraj

Dane wprowadzone na szczeblu gminnym powodują automatycznie wypełnienie formularza na szczeblu powiatowym, wojewódzkim i krajowym.

Moduł musi wspierać informowanie o aktualnym stanie aktualizacji danych
przez poszczególne podmioty. W tym zakresie jego funkcjonalność musi być spięta
z modułem komunikacyjnym w celu możliwości wysłania informacji do podmiotów, które
nie złożyły jeszcze raportu w określonym czasie.

**Moduł administracyjny**

* Lista użytkowników (z możliwością blokady konta, dodawania, edytowania
i kasowania)
* lista użytkowników zalogowanych (musi umożliwiać wyświetlanie aktualnie zalogowanych użytkowników z następującą informacją: (imię i nazwisko, nazwa instytucji, login, adres IP z którego nastąpiło logowanie, data i godzina zalogowania. Musi istnieć możliwość wyeksportowania aktualnej listy użytkowników zalogowanych przez administratora do formatu EXCEL lub PDF)
* log systemowy logowania do systemu (musi umożliwiać wyświetlanie użytkowników którzy są i byli zalogowani w systemie w określonym czasie z następującą informacją: (imię i nazwisko, nazwa instytucji, login, adres IP z którego nastąpiło logowanie, data i godzina zalogowania, data i godzina wylogowania. Musi istnieć możliwość wyeksportowania listy przez administratora do formatu EXCEL lub PDF).
* błędy logowania (musi umożliwiać wyświetlanie użytkowników którzy błędnie logowali się w systemie w określonym czasie z następującą informacją: (imię
i nazwisko, nazwa instytucji, login, adres IP z którego nastąpiło logowanie, data
i godzina logowania. Musi istnieć możliwość wyeksportowania listy
przez administratora do formatu EXCEL lub PDF).
* Rejestracja historii dokonywanych zmian danych z uwzględnieniem informacji
o dacie dokonania zmiany oraz użytkowniku, który tego dokonał. Możliwość konfigurowania poziomu szczegółowości rejestracji (zakresu rejestrowanych danych);
* zarządzanie rolami użytkownika (administrator generalny, administratorzy wojewódzcy muszą mieć możliwość tworząc konto użytkownika lub je modyfikując określać zdefiniowaną rolę (user, GCZK, PCZK, służba, szpital, ZRM, WKRM, WCZK, administrator wojewódzki, administrator generalny itp. Z zastrzeżeniem,
że administrator wojewódzki nie może nadawać uprawnień ponad wojewódzkich
i zastrzeżonych dla administratora generalnego.
* Aktualizacja bazy danych sił i środków (system musi umożliwiać zasilanie bazy danych sił i środków danymi w formatach EXCEL, MS Access posiadającymi
albo współrzędne zasobu lub pola adresowe umożliwiające ich geolokalizację. Funkcjonalność dostępna wyłącznie dla generalnego administratora systemu DUW.
	+ Walidacja
	+ Wczytaj zbiór
* Aktualizacja map cyfrowych (system musi umożliwiać podpięcie do systemu nowej aktualizacji zasobu map cyfrowych)
* Aktualizacja danych o ludności (system musi umożliwiać aktualizowanie danych
o ludności zamieszkałej pod określonymi adresami. Dane niezbędne do wykonywania analiz przestrzennych na mapie po zaznaczeniu określonego obszaru).
	+ Walidacja
	+ Wczytaj zbiór
	+ Archiwum aktualizacji
* edycja słownika modułów systemu
	+ modułu zarządzania bazą danych
		- Kategoria sił i środków
		- Siły i środki
			* rodzaj
			* typ
		- Budowle ochronne
			* budowle ochronne
			* konstrukcje budowli ochronnej
			* lokalizacja budowli ochronnej
			* stan budowli ochronnych
			* status budowli ochronnej
			* typ budowli ochronnej
			* użytkowanie budowli ochronnych
			* własność budowli ochronnej
			* uwagi
		- środki chemiczne
		- centrale alarmowe i syreny darmowe
		- likwidacja skażeń
		- magazyny
		- magazyny przeciwpowodziowe
		- typ nakładu
		- stan techniczny
		- zabezpieczenie w wodę
		- zabytki
	+ modułu administracji
	+ modułu analiz skażeń chemicznych
	+ modułu WKRM, szpitala i ZRM
	+ typ analizy
* Mechanizm replikacji danych zapisanych w bazie operacyjnej do bazy testowej i treningowej. Replikowane muszą być wszystkie dane niezbędne
do funkcjonowania aplikacji Systemu, takie, jak słowniki, dane GIS, dane
o podmiotach i użytkownikach, itp. Administrator generalny powinien mieć możliwość wybrania danych do replikacji przynajmniej na poziomie kategorii (dane GIS, słowniki, itp.) Funkcja dostępna tylko dla administratora generalnego.

 **Administrator generalny musi mieć możliwość definiowania polityki haseł
dla wszystkich użytkowników systemu.**

 W polityce haseł administrator generalny może ustawić:

* minimalną długość hasła
* maksymalny okres ważności hasła liczony w dniach
* określenie liczby historii haseł które nie mogą się powtórzyć
* ustawienie ilości nieudanych prób logowania po których konto zostanie zablokowane
* czas trwania blokady konta

**Kalendarz przedsięwzięć cyklicznych, doraźnych i bieżących**

* kalendarz
	+ dzień
	+ tydzień
	+ miesiąc
	+ rok
* czynności cykliczne
* czynności doraźnie
* czynności bieżące

Moduł ten musi umożliwiać planowanie czynności stałych powtarzających się cyklicznie, czynności doraźnych wynikających z toku pełnienia dyżuru oraz innych czynności bieżących. Moduł musi umożliwiać zaplanowanie realizacji zadań z półtorarocznym wyprzedzeniem
w stosunku do bieżącej daty. Moduł musi działać na zasadzie **“żółtej karteczki”.**Jego położenie powinno znajdować się nad mapą operacyjną w prawym górnym rogu
i rozwijać się po kliknięciu na zakładkę. Moduł musi być spięty z funkcją przypominania
o terminach realizacji zadań.

**Moduł WKRM** (Wojewódzkiego Koordynatora Ratownictwa) musi umożliwiać:

* Bieżące zdarzenia WKRM
* Raporty
* Szpitale z zaległymi raportami
* Szpitale raportujące
* Raport dyżurów pracowni
* Raport szpitali
* Raport zdarzeń WKRM
* Archiwum zdarzeń WKRM
* Baza telefonów do szpitali
* Baza telefonów do dyspozytorni medycznych
* Pokaż łóżka - wyszukiwanie wolnych łóżek (wg kryterium nazwy szpitala, miejscowości, powiatu, województwa, oddziału szpitalnego, minimalnej ilości łóżek
i wszystkich zaznaczonych kryteriów jednocześnie)
	+ W województwie
	+ W wybranych województwach
	+ W kraju

**Moduł Szpital**

* Złóż raport
* Przeglądaj raporty
* Archiwum raportów
* Dane szpitala
* Możliwości jednostki
* Oddziały
* Siły i środki
* Telefony
* Pracownie
* Wyposażenie
* Wyszukiwanie wolnych łóżek
	+ W województwie
	+ W wybranych województwach
	+ W kraju

**Moduł ZRM**

* Wyszukiwanie wolnych łóżek (wg kryterium nazwy szpitala, miejscowości, powiatu, województwa, oddziału szpitalnego, minimalnej ilości łóżek i wszystkich zaznaczonych kryteriów jednocześnie)
	+ W województwie
	+ W wybranych województwach
	+ W kraju

**Moduł HELP**

* Wszystkie objaśnienia, słowa kluczowe i podpowiedzi powinny być w języku polskim;
* System pomocy powinien być wywoływany za pomocą myszy lub po naciśnięciu klawisza F1;
* Każda ikonka na belkach narzędziowych powinna być opatrzona krótkim opisem;
* Każde okno dialogowe powinno posiadać pomoc kontekstową (wywoływaną
jak wyżej) zawierającą znaczenie wszystkich pól i przycisków znajdujących się w tym oknie;
* Musi być dostępny skorowidz tematyczny zawierający wszystkie słowa kluczowe
oraz możliwość szybkiego pozycjonowania w tym skorowidzu (pozycjonowanie
po wpisaniu kolejnych liter klucza);
* Wykonawca powinien zapewnić możliwość tworzenia specjalnej listy - dostępnej
z menu głównego, która zawierać będzie odpowiedzi na najczęściej zadawane pytania (FAQ). Lista ta, redagowana w WCZK, musi być dostępna dla wszystkich użytkowników systemu.

**AD.2 Aplikacja treningowa**

Posiada te same funkcjonalności co Aplikacja Operacyjna z wyłączeniem:

* Publikacji na portalu informacyjnym
* Publikacji w RSO
* Wysyłania SMS
* Raportowania o dostępnej bazie łóżkowej (umożliwia tylko wyszukiwanie łóżek
jak w aplikacji operacyjnej)
* Nie posiada modułu ZRM
* W module szpital ma wyłącznie:
	+ wyszukiwanie łóżek w szpitalach,
	+ wyszukiwanie pracowni i wyposażenia
* W module WKRM posiada wyłącznie
	+ wyszukiwanie łóżek w szpitalach,
	+ wyszukiwanie pracowni i wyposażenia

Aplikacja treningowa posiada w chwili zainstalowania kopię rzeczywistej bazy danych
z możliwością jej okresowej aktualizacji przez administratora generalnego z aplikacji operacyjnej.

Aplikacja treningowa musi posiadać moduł planowania ćwiczeń i treningów dostępną
po przydzieleniu takiego uprawnienia przez administratora generalnego systemu:

* + Tworzenie scenariuszy w tym terminów ich automatycznego i ręcznego uruchamiania
	+ Wprowadzania zdarzeń z terminami ich publikacji w systemie i przypisywania ich do założonych scenariuszów
	+ Modyfikacji scenariuszy i zdarzeń
	+ Archiwum przeprowadzonych treningów i ćwiczeń.
	+ Możliwość wydruku zapisanych scenariuszy, zdarzeń i informacji
	z przynależnymi danymi o planowanych terminach i lokalizacji zdarzeń, adresatami jeśli dotyczy to informacji - w formie tabelarycznej.

Aplikacja treningowa musi umożliwiać uruchamianie min. 16 scenariuszy jednocześnie.

Aplikacja treningowa musi umożliwiać jednoczesną pracę 15000 użytkowników on-line
i prowadzenia tych treningów ćwiczeń w 16 województwach jednocześnie.

**AD.3 Aplikacja Testowa** – dostępność wyłącznie dla firmy dostarczającej system
i administratora generalnego systemu musi zawierać wszystkie moduły z aplikacji operacyjnej i treningowej umożliwiające sprawdzenie przygotowanych funkcjonalności nowych aktualizacji systemu włącznie z publikacją informacji do RSO i PI, SMS, FAX.

**AD.4 Portal Informacyjny** – musi być dostosowany do dostępu dla osób niedowidzących, tj. zgodność z wymogami WCAG 2.0 na poziomie AA (Dz.U. 2019 poz.848 Ustawa z dnia
4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych).

Portal Informacyjny powinien być wyposażony w mechanizmy zabezpieczające, takie jak:

* + zabezpieczenie dostępu do panelu administracyjnego poprzez połączenie szyfrowane
	+ ochrona przed próbami nieautoryzowanego dostępu
	+ odporność na próby uzyskania dostępu poprzez znane formy włamań
	+ odporność na zmiany treści za pomocą specjalnych skryptów

Administrator Portalu Informacyjnego musi mieć pełną możliwość:

1. zarządzania użytkownikami (redaktorami) i ich uprawnieniami
2. pełnego nadzoru nad zawartością merytoryczną i wyglądem Portalu
3. generowania statystyk odsłon pojedynczych stron Portalu; monitorowania poprawności działania serwisu oraz rejestrowania i raportowania aktywności użytkowników

Portal Informacyjny musi być spięty z Aplikacją Operacyjną z której będą wysyłane informacje o zdarzeniach, alarmach, ostrzeżeniach, czasokresie ich obowiązywania. Informacje te oprócz treści muszą się geolokalizować i wyświetlać na mapie cyfrowej Portalu Informacyjnego w zdefiniowanym przedziale czasu. Publikowane w PI informacje muszą mieć możliwość wstawiania załączników w postaci mapek hiperłączy itp. wprowadzanych bezpośrednio na stronę PI przez uprawnionego administratora wojewódzkiego
lub administratora generalnego systemu w części przeznaczonej dla określonego województwa.

Portal informacyjny musi przechowywać całą historię publikacji.

**AD.5 Aplikacja OFFLINE dotyczy wyłącznie obsługi bazy danych sił i środków
na komputerze lokalnym** dla użytkownika systemu z uprawnieniami w zakresie jej obsługi przysługującymi tylko temu użytkownikowi.

Aplikacja OFFLINE musi posiadać lokalnie zainstalowane moduły mapowe na których będą się wizualizować wyszukiwane przez użytkownika zasoby. Aplikacja musi umożliwiać aktualizowanie danych wprowadzonych w trybie OFFLINE okresowo co 1 miesiąc
w zadanych przez administratora generalnego systemu terminach lub na żądanie użytkownika, który wprowadził dane w t~~r~~ym trybie.

**CZĘŚĆ TECHNICZNA**

W związku z tym, że System będzie wykorzystywany przez podmioty związane
z zarządzaniem kryzysowym to musi działać 24/7. Zaprojektowane rozwiązanie technologicznie winno zapewniać bezpieczną i wydajną pracę w systemie dla ok. 45 000 użytkowników oraz musi być tak dobrane, by umożliwiało jednoczesną, wydajną
i bezawaryjną pracę 15 000 użytkowników. Pod pojęciem wydajna rozumie się takie działanie Systemu, w którym czas wykonania dowolnego, predefiniowanego zapytania nie może być dłuższy niż 3 sekundy, a w przypadku wykonania analiz i niestandardowych raportów użytkownik widzi stan realizacji w postaci graficznej.

Zamawiający zakłada budowanie Systemu w dwóch istniejących serwerowniach, zlokalizowanych we Wrocławiu i Poznaniu, gdzie będzie zapewnione zasilanie
wraz z podtrzymaniem i chłodzenie. W serwerowni we Wrocławiu znajduje się pusta szafa rack 47U a do serwerowni w Poznaniu Wykonawca musi dostarczyć szafę rack 42U. Dostarczana szafa do Poznania musi być wyposażona w system kontroli dostępu. System kontroli dostępu musi być dostępny z poziomu sieci LAN tak, aby można było nadawać uprawnienia dostępu i prowadzić rejestr otwarcia szaf. Dodatkowo system musi być wyposażony w czytniki kart zbliżeniowych.

Serwerownia we Wrocławiu będzie serwerownią główną, posiadającą wersję operacyjną Systemu, wersję testową, treningową i Portal Informacyjny. Serwerownia zapasowa ma mieć wersję operacyjną Systemu, aplikację treningową i Portal Informacyjny.

Wykonawca musi też zapewnić redundantne łącza internetowe do każdej lokalizacji.
Przy infrastrukturze krytycznej łącza internetowe powinny być symetryczne i redundantne
o przepustowości min. 10 Gbps w każdej lokalizacji i powinny posiadać publiczną adresację IP. Wykonawca powinien zaprojektować całą adresację IP i przedstawić w projekcie schemat połączeń poszczególnych elementów systemu wraz z informacją w jakim segmencie sieci będzie znajdować się dany element.

Dla dostępności Systemu musi być utworzona infrastruktura sprzętowo – programowa
w jednej jak i w drugiej lokalizacji tak, by przy awarii serwerowni głównej System w wersji operacyjnej i Portal Informacyjny mógł działać z serwerowni zapasowej. W celu osiągnięcia wysokiego poziomu niezawodności komunikacyjnej wszystkie elementy infrastruktury powinny być redundantne. Dobór sprzętu i konfiguracja urządzeń musi umożliwiać dołożenie nowych elementów bez konieczności rekonfigurowania całego środowiska. Przełączanie pomiędzy serwerowniami musi być realizowane „w locie” tzn. w czasie nie dłuższym
jak jedna minuta, a wymiana aktualizacja przyrostowa danych pomiędzy serwerownią główną i zapasową musi być realizowana na bieżąco, tak by realna strata danych nie obejmowała czasu większego jak dwie minuty, wliczając w to czas przejęcia ruchu przez system posadowiony w serwerowni zapasowej.

Przejście do ponownego trybu pracy przez serwerownię główną musi być realizowane
w trybie działania administratora generalnego systemu, który po sprawdzeniu, że serwerownia odtworzyła pełną gotowość do przejęcia pracy zsynchronizowała dane z serwerowni zapasowej.

W lokalizacji serwerowni głównej (Wrocław) muszą funkcjonować i być zainstalowane:

* Aplikacja Operacyjna
* Aplikacja Treningowa
* Aplikacja Testowa
* Portal Informacyjny

W lokalizacji serwerowni zapasowej (Poznań) muszą funkcjonować i być zainstalowane:

* Aplikacja Operacyjna
* Aplikacja Treningowa
* Portal Informacyjny

Ważnym elementem jest tutaj bezpieczeństwo czyli zaprojektowanie zaawansowanych mechanizmów zabezpieczających takich jak firewalle next genaration, systemy antywirusowe i wykrywające ataki, szyfrowane połączenia do systemu, wymuszanie zmiany haseł, stosowanie haseł zgodnych z regułami, podwójne uwierzytelnianie administratorów
w połączeniach VPN/SSL, itp. W infrastrukturze w serwerowni głównej i zapasowej powinien zostać wdrożony wydzielony mechanizm uwierzytelniania administratorów
na urządzeniach i serwerach, system logowania zdarzeń. Dostęp do urządzeń i serwerów musi odbywać się za pomocą kanałów szyfrowanych. Logi ze zdarzeń muszą być przechowywane przez minimum dwa lata. Uruchomione usługi związane z mechanizmem logowania, podwójnej autentykacji oraz uwierzytelnianie administratorów muszą znajdować się wewnątrz infrastruktury zamawiającego.

Ponadto należy zaprojektować metodę/sposób wymiany danych pomiędzy serwerowniami
w trybie online, działania w sytuacjach awaryjnych i w momencie zwiększonego obciążenia Systemu.

Biorąc pod uwagę to, że ma być to System autonomiczny czyli system budowany
na niezależnej platformie sprzętowo-programowej  to musi uwzględniać wszystkie elementy sprzętowe i programowe,  niezbędne do działania i utrzymania systemu oraz Wykonawca winien przewidzieć realizację backupów całego Systemu (backupy baz danych, serwerów, urządzeń sieciowych, itd.) i zaplanować przestrzeń na składowanie kopii bezpieczeństwa.

Zamawiający wymaga też opracowania planu (schematów) testów akceptacyjnych do odbioru Systemu, które obejmowałyby testy funkcjonalne, testy wydajnościowe, testy bezpieczeństwa aplikacji, infrastruktury, itp.

Zamawiający wymaga, aby Wykonawca zaprojektował i dostarczył sprzęt fabrycznie nowy, nieużywany we wcześniejszych projektach, pochodzących z legalnego kanału sprzedaży producentów na rynek europejski oraz był wyprodukowany w bieżącym roku i nie był przeznaczony przez producenta do wycofania z produkcji lub sprzedaży. Wraz z dostawą sprzętu powinien być dostarczony dokument, poświadczający datę produkcji sprzętu (Zamawiający zastrzega sobie prawo weryfikacji legalności sprzętu i licencji u producenta poprzez weryfikację numerów seryjnych).

**CZĘŚĆ USŁUGA UTRZYMANIA**

Zadaniem Wykonawcy będzie świadczenie usługi, zapewniającej ciągłość sprawnego działania Systemu poprzez ciągły monitoring 24/7 wszystkich elementów systemu, wykonywanie cyklicznych przeglądów, aktualizacji systemów operacyjnych, oprogramowania oraz aktualizowanie i serwisowanie zakupionego sprzętu, a także realizację działań naprawczych wynikających z analizy ujawnionych problemów, wykrytych błędów
i wad systemów, niewłaściwego działania Systemu, spadku wydajności, itp. Aktualizacje krytyczne winny być zainstalowane nie później niż 24h od publikacji.

**CZEŚĆ SZKOLENIA**

Zadaniem Wykonawcy będzie przeprowadzenie w terminie do 30.03.2022 r. szkoleń dla min. 300 użytkowników Systemu, wskazanych przez Zamawiającego w lokalizacjach siedzib
11 urzędów wojewódzkich.

**CZĘŚĆ AUDYT BEZPIECZEŃSTWA**

Celem przeprowadzenia audytu jest zweryfikowanie czy wdrożone w ramach projektu rozwiązania informatyczne oraz konfiguracja infrastruktury spełnia wymogi w zakresie obowiązujących w Polsce przepisów prawa i przyjętych dobrych praktyk w zakresie bezpieczeństwa IT.

Przed rozpoczęciem audytu należy ustalić z Zamawiającym akceptowalny poziom zabezpieczeń Systemu.

Zakres prac obejmuje audyt aplikacji, Portalu Informacyjnego oraz infrastruktury teletechnicznej.

Audyt bezpieczeństwa powinien zostać wykonany poprzez analizę i ocenę architektury i konfiguracji poszczególnych komponentów na poziomie dokumentacji oraz bezpośrednio
w środowisku informatycznym Zamawiającego.

Testy powinny być wykonywane z lokalizacji Zamawiającego z wyłączaniem testów badających interfejsy na styku z siecią Internet od strony zewnętrznej, które mogą być prowadzone zdalnie z lokalizacji Wykonawcy.

Wykonawca jest zobowiązany do:

1. opracowania szczegółowego planu przeprowadzenia audytu
2. przeglądu architektury Systemu pod kątem identyfikacji ewentualnych podatności bezpieczeństwa
3. przeprowadzenia audytu w obszarze zgodności z wymogami WCAG 2.0 na poziomie AA Platformy Informacyjnej
4. zbadanie rzeczywistego poziomu bezpieczeństwa informacji oraz zastosowanych zabezpieczeń, a także zgodności tego poziomu z wymaganiami określonymi w normie PN-ISO/IEC 27002
5. przeprowadzenie audytu w obszarze zgodności z wymogami KRI
6. przeprowadzenia audytów bezpieczeństwa informacji dla Systemu oraz Portalu Informacyjnego oraz wskazania zagrożeń i podatności a także ocena aktualnego poziomu bezpieczeństwa
7. przeglądu kodu pod katem identyfikacji ewentualnych podatności bezpieczeństwa
8. przeprowadzenia audytu polityki kopii zapasowych i backup-ów
9. audytu procedur ciągłości działania Systemu na wypadek awarii
10. przeprowadzenia testów weryfikujących poprawność procedur ciągłości działania
na wypadek awarii
11. przeprowadzenia testów penetracyjnych infrastruktury i aplikacji
12. przeprowadzenia testów wydajnościowych i obciążeniowych
13. symulacja ataków cybernetycznych na infrastrukturę sieciowo-serwerową w celu zidentyfikowania podatności.

Produktem końcowym powinien być Raport z Audytu Bezpieczeństwa, zawierający obserwacje oraz rekomendacje Wykonawcy, dotyczące sposobów obniżenia podatności
do akceptowalnego stanu. Po usunięciu podatności winna być weryfikacja i ponowne opracowanie raportu z retestów aż do uzyskania uzgodnionego poziomu zabezpieczenia Systemu.

Raport z Audytu Bezpieczeństwa powinien zawierać następujące pozycje:

# Wstęp - zakres wykonanych prac audytowych.

# Wykaz osób realizujących testy - z uwzględnieniem nazwisk osób odpowiedzialnych za wykonanie badań, przeprowadzenie analizy wyników, opracowanie i kontrolę jakości dokumentacji.

# Termin, miejsce i rodzaj prowadzonych prac audytowych.

# Streszczenie dla kierownictwa zawierające:

* 1. Informacje o komponentach Systemu poddanych testom bezpieczeństwa.
	2. Syntetyczny opis prowadzonych prac audytowych.
	3. Zestawienie zidentyfikowanych podatności i słabości ze wskazanym poziomem ryzyka oraz krótką charakterystykę podatności i słabości o krytycznym lub wysokim poziomie ryzyka, uszeregowanych od najbardziej do najmniej krytycznych.

# Szczegółowa część techniczna zawierająca:

* 1. Opis zastosowanej metodyki.
	2. Wykaz sprawdzonych obszarów, zadań wykonywanych przy sprawdzeniu poszczególnych obszarów wraz ze statusem wykonania zadań, zawierający również rodzaje przeprowadzonych testów i badań, dla których nie zostały wykryte żadne istotne podatności.
	3. Listę i opis wykrytych podatności i słabości wraz z ich klasyfikacją.

**STOSOWANE SKRÓTY I DEFINICJE**

| Termin / skrót | Objaśnienie |
| --- | --- |
| AdatP-3 | Standard meldunku w systemie SI PROMIEŃ |
| API | (ang. Application Programming Interface) Interfejs programowania aplikacji |
| BDOT | Baza Danych Obiektów Topograficznych |
| Backup | Kopia zapasowa danych służąca do ich odtworzenia w przypadku ich uszkodzenia lub utraty |
| CD KSWSiA | Centrum Dyspozycyjne Krajowego Systemu Wykrywania Skażeń i Alarmowania (Centralny Ośrodek Wykrywania Skażeń i Alarmowania) |
| CZK | Centrum Zarządzania Kryzysowego – określenie dotyczy centrów dowolnego szczebla |
| DUW | Dolnośląski Urząd Wojewódzki we Wrocławiu |
| ERG | Zasady postępowania Ratowniczego |
| GCZK  | Gminne Centrum Zarządzania Kryzysowego |
| GDDKiA | Generalna Dyrekcja Dróg Krajowych i Autostrad |
| GIS | (*ang. Geographic Information System*) –system informacyjny służący do wprowadzania, gromadzenia, przetwarzania i wizualizacji danych geograficznych. Wykorzystywany jest m.in. do wspomagania oceny sytuacji i podejmowania decyzji. |
| GML | (*ang. Geography Markup Language*) – format wymiany danych przestrzennych |
| GOPR | Górskie Ochotnicze Pogotowie Ratunkowe |
| GUGiK | Główny Urząd Geodezji i Kartografii |
| GUI | (*ang. Graphical User Interface*) – interfejs graficzny użytkownika aplikacji |
| HRW | Harmonogramu Realizacji Wdrożenia |
| IMGW | Instytut Meteorologii i Gospodarki Wodnej |
| JPEG | (*ang. Joint Photographic Experts Group*) – popularny standard skompresowanego pliku grafiki rastrowej |
| KPZK | Krajowy Plan Zarządzania Kryzysowego |
| KRI | Krajowe Ramy Interoperacyjności |
| MGCO | Międzynarodowa Główna Centrala Ostrzegawcza |
| MKOO | Międzynarodowa Komisja Ochrony Odry |
| OSP | Ochotnicza Straż Pożarna |
| PCZK | Powiatowe Centrum Zarządzania Kryzysowego |
| PDF | (ang. Portable Document Format) – standardowy format dokumentów opracowany przez firmę Adobe Systems |
| PK HNS | Punkt Kontaktowy (ang. Host Nation Support) cywilna i wojskowa pomoc udzielana wojskom sojuszniczym i organizacjom, które są rozmieszczone, wykonują zadania lub przemieszczają się przez terytorium państwa-gospodarza(państwo przyjmujące) w czasie pokoju, sytuacji kryzysowych i wojny |
| PI | Portal Informacyjny |
| POZK | Portal Operacyjny Zarządzania Kryzysowego – środowisko pracy i współpracy wszystkich CZK, Inspekcji, służb i straży będących użytkownikami systemu |
| PSP | Państwowa Straż Pożarna |
| PTW | Projekt Techniczno-Wykonawczy Systemu  |
| PUWG92 | Państwowy Układ Współrzędnych Geodezyjnych 1992 |
| PUWG2000 | Państwowy Układ Współrzędnych Geodezyjnych 2000 |
| RCB | Rządowe Centrum Bezpieczeństwa |
| RSO | Regionalny System Ostrzegania |
| RZGW | Regionalny Zarząd Gospodarki Wodnej – Wody Polskie |
| SSL | (ang. Secure Socket Layer) – protokół szyfrowanej transmisji umożliwiający bezpieczne przesyłanie danych poprzez Internet |
| SSO | (ang. Single Sign-On)logowanie jednokrotne |
| SWDE | Standard Wymiany Danych Ewidencyjnych |
| System | System Wczesnego Ostrzegania, Alarmowania i Informowania 2.0 |
| TIF lub TIFF | (ang. Tagged Image File Format) – format pliku graficznego dla grafiki rastrowej |
| WCAG | (ang. Web Content Accessibility Guidelines) - zestaw wymagań dotyczących dostępności stron internetowych dla osób niepełnosprawnych. Od wersji 2.0 jest to międzynarodowy standard dla tworzonych serwisów internetowych. |
| WCZK | Wojewódzkie Centrum Zarządzania Kryzysowego we Wrocławiu |
| WGS-84 | (ang. World Geodetic System '84) zbiór parametrów (z 1984 r.) określających wielkość i kształt Ziemi oraz właściwości jej potencjału grawitacyjnego |
| WMS | (ang. Web Map Service) – standard udostępniania map w postaci rastrowej za pomocą interfejsu http |
| WMTS | (ang. Web Map Tile Service) – standard udostępniania map w postaci kafelków za pomocą interfejsu http |
| WOPR  | Wodne Ochotnicze Pogotowie Ratunkowe |
| WPZK | Wojewódzki Plan Zarządzania Kryzysowego |
| WUW | Wielkopolski Urząd Wojewódzki |
| VPN | (ang. *Virtual Private Networ*k) – tunel, poprzez który płynie transmisja danych pomiędzy użytkownikami sieci prywatnej |
| UTM | (ang. Universal Transverse Mercator)  |
| Zakłady DDD | Zakłady zajmujące się Dezynfekcją, Dezynsekcją i Deratyzacją |
| ZDR | Zakład Dużego Ryzyka |
| ZMSz | Zastępcze Miejsca Szpitalne |
| ZRM | Zespół Ratownictwa Medycznego |
| ZZR | Zakład Zwiększonego Ryzyka |