***Załącznik nr 2 do SIWZ***

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

**Opis przedmiotu zamówienia**

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.**

Spis treści

1. Uwagi …………………………………………………………………………………………………………….……… 3
2. Wymagania …………………………………………………………………………………………..………..…….. 4
3. Widok kooperacji systemu ………………………………………………………………………..……….… 23
4. Aplikacja Operacyjna – wymagania ogólne …………………………………………………….……. 24
5. Główne funkcjonalności systemu ………………………………………………………………….…….. 24
	1. Moduł Komunikacyjny ……………………………………………………………………..………. 24
	2. Moduł Operacyjny …………………………………………………………………………….…..…. 31
	3. Moduł Baza Danych Sił i Środków ……………………………………………………………… 39
	4. Moduł Analizy Przestrzenne ……………………………………………………………………… 42
	5. Moduł Obsługi Mapy ………………………………………………………………………………... 43
	6. Moduł Zarządzania Publikacją Informacji Na Zewnątrz Systemu ……………….. 44
	7. Moduł Raportowania ………………………………………………………………………………… 44
	8. Moduł Generator Formularzy Raportowania …………………………….……………… 47
	9. Moduł Obsługi Zdarzeń Chemicznych ……………………………………………………….. 48
	10. Moduł Administracyjny …………………………………………………………………………….. 48
	11. Moduł Kalendarz Przedsięwzięć Cyklicznych, Doraźnych i Bieżących …..……. 51
	12. Moduł WKRM …………………………………………………………………………………………… 52
	13. Moduł Szpital ……………………………………………………………………………………………. 53
	14. Moduł Pogotowie Ratunkowe ………………………………………………………………….. 53
	15. Moduł Help ………………………………………………………………………………………………. 53
6. Aplikacja Treningowa ……………………………………………………………..………………………... 54
7. Aplikacja Testowa ………………………………………………………………………………………………… 55
8. Portal Informacyjny ……………………………………………………………………………………………… 55
9. Aplikacja OFFLINE ………………………………………………………………………………………………… 56
10. Stosowane skróty i definicje ……………………………………………………………………………..…. 57

Uwagi:

**Uwaga 1:** Projekt, który jest przedmiotem niniejszego zamówienia jest projektem typu „Zaprojektuj i Wybuduj”. W „Opisie przedmiotu zamówienia” 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 przedmiotu zamówienia 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.

Wymagania.

**„System Ostrzegania Alarmowania i Informowania 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.**
6. **Przeznaczenie Systemu.**
* 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, analiz przestrzennych i informacji dla ludności, do Regionalnego Systemu Ostrzegania (RSO) i Portalu Informacyjnego (PI).
* 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, w tym z systemu COVID-19 Rządowego Centrum Bezpieczeństwa.
* Możliwość wprowadzania do systemu i wykorzystania, podczas wystąpienia sytuacji kryzysowej, procedur i scenariuszy wynikających z planów 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 – wg parametrów zadanych przez administratora.
* Tworzenie nowych formularzy raportów i przypisywanie uprawnień do ich aktualizowania po zarządzeniu raportowania - poprzez Globalny generator formularzy.

W Systemie zarejestrowanych będzie ok. 45000 kont użytkowników, z tego dla pracy Online należy zapewnić płynny 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. Zamawiający dopuszcza użycie niekomercyjnej bazy danych, ale tylko na potrzeby gromadzenia dużej ilości danych przestrzennych takich jak dane referencyjne typu OSM. Ponadto niekomercyjne silniki bazy danych muszą się charakteryzować brakiem ograniczeń licencyjnych w zakresie procesorów i użytkowników, tym samym pozwalający na instalowanie nowych instancji serwera bazodanowego, posiadać mechanizmy replikacji danych online do zapasowego serwera bazodanowego, być wspieranym przez środowisko serwerów GIS, które będą publikować dane przestrzenne w postaci usług sieciowych. W podejściu hybrydowym dla pełnej jednolitości i spójności stosu technologicznego baz danych koniecznym jest, aby silniki bazodanowe użyte w projekcie posiadały pełną kompatybilność typów przestrzennych. Dodatkowo serwery GIS publikujące usługi mapowe i dane przestrzenne muszą móc jednocześnie korzystać z baz danych umieszczonych na użytych, różnych serwerach bazodanowych.

**Wykonawca, któremu zostanie udzielone zamówienie, będzie musiał wykonać następujące zadania:**

1) Opracowanie Projektu Techniczno - Wykonawczego oraz opracowanie Harmonogramu Realizacji Wdrożenia Systemu

2) Zbudowanie i wdrożenie Systemu

3) Zakup sprzętu, oprogramowania, wymaganych licencji, gwarancji wraz ze wsparciem na okres 5 lat od daty podpisania Protokołu Końcowego Odbioru Prac

4) Wykupienie, w imieniu Zamawiającego, usług dostawy Internetu symetrycznego wraz z publiczną adresacją IP do serwerowni we Wrocławiu i Poznaniu o przepustowości 10 Gb/s, oraz łączy symetrycznych między tymi dwoma lokalizacjami o przepustowości 10 Gb/s na okres 5 lat od daty podpisania Protokołu Końcowego Odbioru Prac

5) Zakup i utrzymanie nazwy domeny w imieniu Zamawiającego

6) Zakup i utrzymanie ważności certyfikatu SSL w imieniu Zamawiającego

7) Montaż, uruchomienie, instalacja oraz konfiguracja sprzętu i oprogramowania w lokalizacjach: Wrocław i Poznań

8) Przeprowadzenie testów akceptacyjnych całego Systemu na podstawie opracowanych przez Wykonawcę i zaakceptowanych przez Zamawiającego scenariuszy testów

9) Przeprowadzenie szkoleń

10) Opracowanie i dostarczenie wszystkich wymaganych instrukcji dla Administratorów i Użytkowników Systemu

11) Opracowanie i dostarczenie dokumentacji powykonawczej Systemu

12) Przeprowadzenie audytu bezpieczeństwa i uzyskanie akceptowalnego poziomu zabezpieczenia Systemu z audytu bezpieczeństwa

13) Opracowanie metody badania analizy ryzyka Systemu i przeprowadzenie tej analizy

14) Opracowanie planu ciągłości działania Systemu

15) Przekazanie Zamawiającemu kodów źródłowych do wytworzonych aplikacji

16) Przekazanie Zamawiającemu wszelkich licencji związanych z Systemem

17) Przekazanie Zamawiającemu wszelkich gwarancji związanych z Systemem

18) Nieodpłatne świadczenie usługi utrzymania całego Systemu przez okres 5 lat od daty podpisania Protokołu Końcowego Odbioru Prac

**AD 1)**

Projekt Techniczno – Wykonawczy (PTW) winien być wykonany w oparciu o wymagania określone w SIWZ, ofercie Wykonawcy oraz w wyniki analiz i uzgodnień z Zamawiającym. PTW będzie aktualizowany w trakcie trwania Projektu.

Harmonogramu Realizacji Wdrożenia (HRW) winien zawierać wyszczególnienie „kamieni milowych” wdrożenia oraz dat ich osiągnięcia.

Zatwierdzenie PTW i HRW przez Zamawiającego będzie pozwalało na dalszą realizację zadania

**AD 2)**

**Szczegółowy opis poszczególnych zadań podany jest w kolejnych rozdziałach Opisu przedmiotu zamówienia (od punktu widok kooperacji systemu).**

**AD 3)**

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 praca 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 w 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. Szafa rack 19” do serwerowni w Poznaniu musi mieć wymiary 600x1000mm, być w kolorze czarnym oraz posiadać perforowane drzwi z przodu i tyłu. W serwerowni w Poznaniu znajdują się szafy rack firmy Linkbasic P/N: NCB42-610-IFA-C dla zapewnienia jednolitości infrastruktury zamawiający wymaga zakupu powyższej szafy lub równoważnej. Dostarczana szafa do Poznania musi być wyposażona w system kontroli dostępu wraz z czytnikiem kart zbliżeniowych i czteroma kartami zbliżeniowymi. System kontroli dostępu musi być dostępny z poziomu sieci LAN tak, aby można było nadawać uprawnienia dostępu i prowadzić rejestr otwarcia szaf. Ponadto system kontroli dostępu musi być objęty centralnym systemem kopii zapasowych oraz musi umożliwiać zapisywanie logów do centralnego serwera logów. Szafę teleinformatyczną w Poznaniu trzeba wyposażyć w europejskie listwy zasilające, a szafa we Wrocławiu posiada dwie listwy zasilające po około 15 gniazd C13.

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, treningowej i Portal Informacyjny mógł działać z serwerowni zapasowej. W celu osiągnięcia wysokiego poziomu niezawodności komunikacyjnej wszystkie elementy infrastruktury muszą 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. Ponadto Zamawiający wymaga, aby była możliwa alternatywna konfiguracja mechanizmu przełączania się pomiędzy serwerowniami poprzez ręczne sterownie. Scenariusz przełączania pomiędzy serwerowniami zostanie ustalony na etapie projektowania.

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

Wszystkie urządzenia, które będą wykorzystywane w projekcie muszą mieć możliwość zamontowania w standardowej szafie rack 19” oraz muszą być wyposażone w niezbędne komponenty do montażu. Wkładki optyczne będące częścią składową urządzeń sieciowych muszą być certyfikowane przez producenta, chyba że producent dopuszcza użycie wkładek firm trzecich bez utraty wsparcia serwisowego oferowanych urządzeń. Do urządzeń należy dołączyć kable zasilające, patchcordy oraz wkładki światłowodowe o maksymalnej przepustowości portu do którego zostaną wsadzone w ilościach niezbędnych do podłączenia całej infrastruktury.

Oferowane serwery muszą posiadać co najmniej dwie karty sieciowe po dwa porty o przepustowości 10 Gb/s, dwie karty FC po minimum jednym porcie 32Gb/s, dwa zasilacze redundantne typu Hot-Plug, dyski SSD typu Hot-Plug oraz minimum dwa redundantne wentylatory typu Hot-Plug. Ponadto serwery muszą wspierać system wirtualizacji oferowany przez Wykonawcę.

Wykorzystywane serwery muszą być wyposażone w kartę zdalnego zarządzania (konsoli) wyposażoną w dedykowaną kartę sieciową 1 Gb pozwalającą na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Karta musi także umożliwiać przejęcie zdalnej konsoli graficznej i podłączanie wirtualnych napędów CD/DVD/ISO i USB. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe dedykowanym/PCI w komplecie z wymaganymi licencjami. Dodatkowo karta musi umożliwiać zapis logów do centralnego serwera logów oraz monitorowanie stanu serwera za pomocą protokołu SNMP.

Oferowane macierze dyskowe muszą posiadać podwójny kontroler Active-Active lub Active-Passive. Kontrolery w klastrze wysokiej dostępności muszą oferować funkcjonalność automatycznego przejmowania funkcjonalności i zadań w przypadku awarii drugiego kontrolera w tej samej parze. Kontrolery muszą mieć możliwość wymiany podczas pracy. Każdy z kontrolerów macierzy musi być wyposażony w co najmniej dwa porty FC o przepustowości minimum 32Gb/s i jeden port minimum 100 BaseTX do obsługi protokołów zarządzania. Macierze dyskowe mogą być wyposażone w dyski NVMe, SSD/Flash lub SAS w takich ilościach oraz typach aby zapewnić wydajne działanie systemu. Dodatkowo macierze muszą umożliwiać zapis logów do centralnego serwera logów oraz monitorowanie stanu za pomocą protokołu SNMP. Macierze muszą zapewniać jak najwyższą niezawodność poprzez zastosowanie redundantnych zasilaczy, redundantnego chłodzenia, kontrolerów, dwóch ścieżek dostępu do każdego dysku – po jednej ścieżce z każdego kontrolera. Dyski, zasilacze, kontrolery oraz chłodzenie muszą mieć możliwość wymiany podczas pracy macierzy. Konfiguracja przestrzeni dyskowej macierzy musi zapewniać funkcjonalność udostępniania przestrzeni bez konieczności fizycznego alokowania wolnego miejsca na dyskach (thin provisioning). Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla wszystkich macierzy w maksymalnej konfiguracji. Macierze muszą obsługiwać LUN Masking. Sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu powinny być dostępne dla podłączanych systemów operacyjnych. Jeżeli zastosowanie tych sterowników wymaga licencji, muszą być dostarczone dla podłączanych systemów operacyjnych. Macierze muszą posiadać funkcjonalność zwiększania rozmiaru wolumenów. Macierze muszą zapewniać wykonywanie kopii migawkowych. Przepełnienie przestrzeni dla kopii migawkowych nie może powodować błędów zapisu na przestrzeń produkcyjną. Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest obecnie przedmiotem zamówienia. Macierze muszą wspierać mechanizm zdalnej replikacji z poziomu macierzy na drugą macierz, w trybie co najmniej asynchronicznym. Replikacja danych pomiędzy macierzami nie może być realizowana zewnętrznym narzędziem software'owym. Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest przedmiotem zamówienia.

Przełączniki do sieci SAN muszą być wykonane w technologii FC i zapewniać w dostarczonej konfiguracji możliwość pracy portów FC z prędkościami 32, 16, 10, 8, 4 Gb/s w zależności od typu zainstalowanych wkładek SFP. Przełączniki muszą mieć redundantne zasilacze typu Hot-Plug oraz wentylatory typu Hot-Plug. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego. Przełączniki musza umożliwiać definiowanie kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP. Przełącznik musi zapewnić możliwość jego zarządzania przez dedykowany port Ethernet. Dodatkowo przełączniki muszą umożliwiać zapis logów do centralnego serwera logów oraz monitorowanie stanu za pomocą protokołu SNMP.

Oferowane przełączniki rdzeniowe muszą zapewniać przepustowość interfejsów sieciowych na poziomie minimum 10 Gb/s. Urządzenia muszą posiadać możliwość zdefiniowania, co najmniej 1000 aktywnych sieci VLAN oraz umożliwić nadanie numeru VLAN do 4094 (ID VLAN). Urządzenia muszą umożliwiać zapisanie na pamięci Flash co najmniej dwóch wersji systemu operacyjnego. Urządzenia muszą wspierać następujące standardy warstwy 2: 802.3(vlan), 802.3ad(LAG), 802.1p, 802.1q, 802.1d, QinQ pass-through, Jumbo Frames . Przełączniki muszą mieć redundantne zasilacze typu Hot-Plug oraz wentylatory typu Hot-Plug. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego. Przełączniki musza umożliwiać definiowanie kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP. Dodatkowo przełączniki muszą umożliwiać zapis logów do centralnego serwera logów oraz monitorowanie stanu za pomocą protokołu SNMP. Urządzenia muszą wspierać następujące mechanizmy związane z zarządzaniem: SSHv2, port konsoli, dedykowany port Ethernet do zarządzania out-of-band.

Oferowane przełączniki do podłączenia sieci zarządzającej muszą zapewniać przepustowość interfejsów sieciowych na poziomie minimum 1 Gb/s. Urządzenia muszą posiadać możliwość zdefiniowania, co najmniej 1000 aktywnych sieci VLAN oraz umożliwić nadanie numeru VLAN do 4094 (ID VLAN). Urządzenia muszą wspierać następujące standardy warstwy 2: 802.3(vlan), 802.3ad(LAG), 802.1p, 802.1q, 802.1d, QinQ pass-through, Jumbo Frames. Urządzenia muszą umożliwiać zapisanie na pamięci Flash co najmniej dwóch wersji systemu operacyjnego. Przełączniki muszą mieć redundantne zasilacze typu Hot-Plug. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego. Przełączniki musza umożliwiać definiowanie kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP. Dodatkowo przełączniki muszą umożliwiać zapis logów do centralnego serwera logów oraz monitorowanie stanu za pomocą protokołu SNMP. Urządzenia muszą wspierać następujące mechanizmy związane z zarządzaniem: SSHv2, port konsoli, dedykowany port Ethernet do zarządzania out-of-band.

Ważnym elementem jest bezpieczeństwo czyli zaprojektowanie zaawansowanych mechanizmów zabezpieczających takich jak:

* zapory sieciowe nowej generacji tzw. Next Generation Firewall z możliwością filtrowania ruchu po geolokalizacji tzw. GeoIP Filtering wraz z niezbędnymi licencjami.
* urządzenia, służące do rozdzielenia ruchu sieciowego ang. load balancer z wbudowaną zaporą sieciową ze ścisłym przeznaczeniem do ochrony aplikacji webowych tzw. Web Application Firewall wraz z niezbędnymi licencjami.
* system antywirusowy wspierający oferowany system wirtualizacji.
* szyfrowane połączenia do systemu
* wymuszanie zmiany haseł, stosowanie haseł zgodnych z regułami
* podwójne uwierzytelnianie administratorów w połączeniach VPN/SSL np. poprzez potwierdzenie powiadomienia w aplikacji na urządzeniach Android lub iOS.

Oferowane zapory sieciowe muszą zapewniać przepustowość interfejsów sieciowych na poziomie minimum 10 Gb/s. Zapory sieciowe oprócz klasycznej roli zapory ogniowej, filtracji antywirusem, IPS, będą pełniły rolę koncentratorów VPN. Ponadto muszą mieć możliwość zdefiniowania kilku stref np. Strefy DMZ, w której będą pracowały serwery aplikacyjne. W serwerowniach muszą być zainstalowane po dwie zapory sieciowe, które będą pracowały w klastrze active-active lub active-passive (tryb pracy zostanie ustalony podczas tworzenie projektu). Autentykacja użytkowników zapory sieciowej musi odbywać się za pomocą protokołów MS Active Directory, LDAP, Radius. Zapory sieciowe muszą mieć redundantne zasilacze typu Hot-Plug.

Zamawiający wymaga, aby urządzenia, które będą terminowały łącza internetowe posiadały obsługę protokołu routingu BGP (Border Gateway Protocol).

Dla zwiększenia poziomu dostępu do aplikacji oraz poziomu bezpieczeństwa Zamawiający wymaga uruchomienia urządzeń do rozdzielenia ruchu sieciowego (ang. load balancer) wraz z zaawansowanym systemem klasy Web Application Firewall. Oferowane load balancery muszą zapewniać przepustowość interfejsów sieciowych na poziomie minimum 10 Gb/s. Urządzenia do rozdzielenia ruchu sieciowego muszą wspierać inspekcje warstwy aplikacji , w tym inspekcje nagłówka http oraz multipleksowanie połączeń http. Zarządzanie regułami bezpieczeństwa musi być realizowane za pomocą wbudowanego w urządzenia interfejsu graficznego. Reguły definiujące ruch muszą zawierać oprócz adresów IP również możliwość wskazania lokalizacji (w ruchu źródłowym oraz ruchu docelowym) tzw. Geolokalizacja. Mechanizm Web Application Firewall musi działać w oparciu o pozytywny model bezpieczeństwa (tylko to, co znane i prawidłowe jest dozwolone), model ten tworzony jest na bazie automatycznie budowanego przez WAF profilu aplikacji Web. Oprócz pozytywnego modelu zabezpieczeń WAF musi posiadać również funkcje identyfikacji incydentów poprzez sygnatury (negatywny model zabezpieczeń). Powinna być możliwość definicji zaufanych adresów źródłowych, z których algorytm tworzenia profilu bezpieczeństwa WAF będzie akceptować wszystkie zachowania jako prawidłowe, tak aby administrator mógł przyspieszyć proces tworzenia profilu bezpieczeństwa. Musi istnieć możliwość ręcznego konfigurowania/modyfikacji reguł polityki bezpieczeństwa. WAF musi posiadać mechanizmy ochrony przed atakami SQL Injection, Cross-Site Scripting, Cross-Site Request Forgery, Session hijacking, Command Injection, Cookie/Session Poisoning, Brute Force Login, Cookie manipulation/poisoning, Buffer Overflow. WAF musi posiadać mechanizmy ochrony przed atakami DDoS lub DoS ukierunkowanymi na warstwę aplikacyjną (zalewanie aplikacji web dużą ilością zapytań http). WAF musi blokować ataki typu Slow Loris. WAF musi umożliwiać blokowanie zapytań z danego obszaru geograficznego. Aktualizacje bazy geolokacyjnej powinny być dostępne w ramach wsparcia, zapewnionego razem z urządzeniami load balacer. Load balacery muszą mieć redundantne zasilacze typu Hot-Plug. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego. Load balacery muszą umożliwiać definiowanie kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP. Dodatkowo Load balacery muszą umożliwiać zapis logów do centralnego serwera logów oraz monitorowanie stanu za pomocą protokołu SNMP. Oferowany loadbalancer musi wspierać mechanizm Global Traffic Manager, jeżeli wymieniona funkcjonalność wymaga licencji to należy ją zakupić.

W infrastrukturze w serwerowni głównej i zapasowej powinien zostać wdrożony wydzielony mechanizm uwierzytelniania administratorów na urządzeniach i serwerach oraz 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 (kopii bezpieczeństwa) całego Systemu (backupy baz danych, serwerów, urządzeń sieciowych, itd.) i zaplanować przestrzeń na składowanie kopii bezpieczeństwa. Zamawiający wymaga, żeby w obydwu lokalizacjach do backupu były dedykowane serwery(wirtualne lub fizyczne) oraz urządzenia dyskowe, posiadające funkcje replikacji. System kopii zapasowych musi pracować w trybie wysokiej dostępności tak, aby obydwa serwery posiadały te same informacje o zadaniach i wykonanych kopiach. Kopie zapasowe muszą być replikowane do lokalizacji w Poznaniu.

Kopie bezpieczeństwa winny być wykonywane:

* + - w cyklu dobowym (w godzinach nocnych) do postaci tzw. kopii przyrostowych, zawierających zapis jedynie tych informacji, które podczas ostatniej doby uległy zmianie;
		- w cyklu tygodniowym tworzony pełny backup systemów łącznie z kopią systemów operacyjnych serwerów;
		- pełne kopie baz danych raz na dobę i kopie logów transakcyjnych co 30 minut
		- kopie konfiguracji urządzeń sieciowych, firewalli, itp. po każdej zmianie w konfiguracji i cyklicznie raz w miesiącu;
		- kopie logów.

Kopia bezpieczeństwa aplikacji testowej może być wykonywana raz w miesiącu trybie pełnej kopii bez kopii przyrostowych.

Kopie bezpieczeństwa powinny być przechowywane na dyskach macierzy backupowej przez minimum 30 dni, a po upływie tego okresu sukcesywnie nadpisywane lub kasowane. Zamawiający planuje wykorzystywać Chmurę Krajową, jako trzecie miejsce trzymania danych. Częstotliwość przesyłania danych na chmurę odbywać się będzie według wytycznych Zamawiającego, ale nie częściej niż raz na miesiąc.

Poprawność wykonania kopii bezpieczeństwa powinna być weryfikowana automatycznie (przez program kopii zapasowych lub inne narzędzia).

W procesie wykonywania kopii bezpieczeństwa powinien być wykorzystywany mechanizm deduplikacji.

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).

**AD 4)**

Wykonawca musi zapewnić redundantne łącza internetowe do każdej lokalizacji oraz wymaganą pulę publicznych adresów IP wraz z numerem autonomicznym dla protokołu BGP. Przy infrastrukturze krytycznej łącza internetowe powinny być symetryczne i redundantne o przepustowości min. 10 Gbps w każdej lokalizacji. Ponadto Wykonawca musi zapewnić redundantne, symetryczne łącza pomiędzy lokalizacjami (Wrocław, Poznań) o przepustowości 10 Gbps dla sprawnej replikacji danych pomiędzy lokalizacjami.

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.

**AD 5)**

Wykonawca musi zakupić i potem zapewnić utrzymanie nazwy domeny wskazanej przez Zamawiającego przez okres 5 lat od daty podpisania Protokołu Końcowego Odbioru Prac. Domena musi posiadać krajowe rozszerzenie pl.

**AD 6)**

Wykonawca musi zakupić i potem zapewnić utrzymanie ważności certyfikatu SSL typu Trusted przez okres 5 lat od daty podpisania Protokołu Końcowego Odbioru Prac

**AD 7)**

System musi być uruchomiony na dwóch klastrach wirtualizacyjnych - jeden we Wrocławiu, drugi w Poznaniu i będą one zarządzane za pomocą serwera zarządzającego. Takie rozwiązanie ma zapewnić wysoką niezawodność w ramach jednej lokalizacji, jednocześnie dając możliwości spójnego monitorowania i zarzadzania oraz wymiany danych między klastrami. Dodatkowo użycie tej technologii ułatwi zarządzanie i wykonywanie kopii zapasowych (kopie migawkowe maszyn wirtualnych) oraz umożliwi wdrożenie mechanizmów zintegrowanego skanowania antywirusem na poziomie maszyny wirtualnej. Na klastrach zostaną uruchomione maszyny wirtualne z systemami operacyjnymi Microsoft Windows Server jak i Linux w zależności od potrzeb.

Serwer zarządzający musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno jako aplikacja na maszynie fizycznej lub wirtualnej, jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory lub LDAP. System do wirtualizacji musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 8 lub więcej takich procesów przenoszenia jednocześnie. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej oraz zapewniać mechanizmy balansowania dla ruchu sieciowego wychodzącego przez fizyczne karty sieciowe. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN). Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z kilku dostępnych ścieżek. Serwer zarządzający musi być wspierany przez oferowany przez wykonawcę system kopii zapasowych.

Dla zwiększenia niezawodności systemu Zamawiający wymaga, aby wykorzystywane w projekcie serwery bazodanowe pracowały w klastrze niezawodności tak, aby w przypadku awarii jednego serwera bazodanowego dostęp do danych automatycznie przełączył się na drugi serwer. Klaster wysokiej dostępności serwera bazodanowego musi być zbudowany w każdej lokalizacji. Replikacja danych z baz danych pomiędzy lokalizacjami musi być realizowana za pomocą wbudowanych funkcji silnika bazodanowego.

**AD 8)**

Zamawiający wymaga też opracowania planu (schematów) testów akceptacyjnych do odbioru Systemu, które obejmowałyby testy funkcjonalne, testy integracyjne (zbudowanych modułów, komponentów i wymiany danych z systemami zewnętrznymi), testy wydajnościowe, testy bezpieczeństwa aplikacji, infrastruktury, itp.

**AD 9)**

Zadaniem Wykonawcy będzie przeprowadzenie szkoleń dla min. 300 użytkowników Systemu, wskazanych przez Zamawiającego w lokalizacjach siedzib 16 urzędów wojewódzkich, w terminie ustalonym w Harmonogramie. Celem szkoleń ma być nabycie wiedzy i umiejętności w zakresie obsługi funkcjonalności aplikacji wspomagających realizację zadań dla użytkowników, administrowania dla administratorów wojewódzkich i administratora generalnego. Szacuje się, że szkolenie dla użytkowników powinno trwać 8 godzin i dla administratorów 8 godzin.

Szkolenie dla użytkowników może być prowadzone w formie prezentacji.

Szkolenie dla administratorów winno być prowadzone w formie warsztatów w siedzibie Zamawiającego, w terminie ustalonym w Harmonogramie, na środowisku testowym i winno obejmować:

* architekturę Systemu
* ogólne zasady pracy Systemu oraz otoczenia aplikacji, współpracy z innymi aplikacjami
* omówienie ról i zadań użytkowników
* procedury administrowania, w tym także monitorowania środowiska i backupu
* narzędzia wspierające administrowanie, zarządzanie infrastrukturą techniczną
* wiedzę niezbędną do wykonywania diagnozy incydentów i ich zgłaszania do Wykonawcy

**AD 10)**

Instrukcja dla Użytkowników powinna zawierać informacje, które są niezbędne do samodzielnego i sprawnego wykonywania wszelkich operacji przez Użytkownika w pracy z Systemem

Instrukcja dla Administratorów powinna zawierać co najmniej następujące informacje:

* procedury administracyjne
* procedury zabezpieczeń (backup'owe)
* procedury awaryjne
* procedury Użytkownika
* procedura całkowitego odtworzenia systemu (uruchomienie systemu od podstaw)
* procedura przełączania pomiędzy serwerowniami na wypadek awarii i testów.

Instrukcje powinny być przekazane przed szkoleniami z kilkudniowym wyprzedzeniem.

Instrukcje dla Użytkowników mogą być przekazane do Zamawiającego w formie elektronicznej (wersja edytowalna i pdf).

Instrukcja dla Administratorów powinna być przekazana do Zamawiającego w wersji papierowej (2 kopie) i elektronicznej (wersja edytowalna i pdf).

**AD 11)**

Dokumentacja powykonawcza powinna spełniać następujące szczegółowe warunki:

* w pełni odzwierciedlać architekturę logiczną i sprzętową Systemu, jej organizację oraz wszystkie funkcje przewidziane do realizowania przez System, w tym administratorów i Użytkowników
* pełną adresację wraz z umieszczeniem elementów w danym segmencie sieci
* schemat logiczny połączeń w utworzonej infrastrukturze
* konfiguracji urządzeń sieciowych (WAN, LAN, SAN), serwerów, macierzy, systemów zarządzania, systemu SIEM, wirtualizacji
* zawierać kompletny i szczegółowy opis przyjętych rozwiązań funkcjonalnych wraz z informacjami o parametrach i sposobie konfiguracji, konstrukcyjnych, użytkowych i sprzętowych, z wyspecyfikowaniem asortymentowym i ilościowym wszystkich elementów składowych Systemu
* określać zasady i plany instalacji, uruchomienia i wdrożenia Systemu
* powinna być dostarczona zarówno w formie wydrukowanej w co najmniej 2 kopiach, jak również w postaci cyfrowej na co najmniej 2 nośnikach w edytowalnych kopiach
* raport z przeprowadzonego audytu bezpieczeństwa
* dostarczenie zestawienia danych identyfikacyjnych (rodzaje i numery seryjne urządzeń, rodzaje i numery seryjne modułów, licencji, wersje oprogramowania, ilość oraz rodzaj pamięci w każdym urządzeniu).

Dokumentacja powykonawcza powinna być przekazana do Zamawiającego w wersji papierowej (2 kopie) i elektronicznej (wersja edytowalna i pdf).

**AD 12)**

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. W związku z tym Wykonawca winien zlecić firmie specjalizującej się w Audytach Bezpieczeństwa przeprowadzenie audytu bezpieczeństwa i dążyć do uzyskania akceptowalnego poziomu zabezpieczenia Systemu .

Przed rozpoczęciem audytu należy ustalić z Zamawiającym akceptowalny poziom zabezpieczeń Systemu. Wykorzystywane oprogramowanie do audytu musi również uzyskać zgodę Zamawiającego.

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 2.1 na poziomie AA Platformy Informacyjnej
4. zbadanie rzeczywistego poziomu bezpieczeństwa informacji oraz zastosowanych zabezpieczeń,
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:

1. Wstęp - zakres wykonanych prac audytowych.
2. Wykaz osób realizujących testy - z uwzględnieniem nazwisk osób odpowiedzialnych za wykonanie badań, przeprowadzenie analizy wyników, opracowanie i kontrolę jakości dokumentacji.
3. Termin, miejsce i rodzaj prowadzonych prac audytowych.
4. 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.
5. 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.

**AD 13)**

Zadaniem Wykonawcy będzie opracowanie metody badania analizy ryzyka Systemu i przeprowadzenie tej analizy. W opracowaniu muszą znajdować się opisy zasobów systemu teleinformatycznego, zagrożenia oddziaływujące na zasoby, podatności zasobów lub zabezpieczeń, a także wskazywać punkty krytyczne i zagrożenia mające wpływ na niezawodne działanie Systemu.

**AD 14)**

Zadaniem Wykonawcy będzie opracowanie Planu Ciągłości Działania Systemu. Dokument powinien zawierać między innymi informacje/procedury dotyczące przełączania z lokalizacji głównej na lokalizacje zapasową, a następnie przywracanie do lokalizacji głównej.

**AD 15)**

Wykonawca musi przekazać Zamawiającemu kody źródłowe do wytworzonych aplikacji: operacyjnej, treningowej, testowej, Portalu Informacyjnego oraz Aplikacji OFFLINE.

Wykonawca musi również przekazać Zamawiającemu uprawnienia administracyjne do wszystkich elementów Systemu poprzez przekazanie takich danych jak: login i hasło. Dane te będą w zabezpieczonych przed otwarciem kopertach i zdeponowane u Zamawiającego. W związku z tym, że Wykonawca odpowiada za utrzymanie całego Systemu to dane te nie będą wykorzystywane w trakcie umowy.

**AD 16)**

Wykonawca musi udzielić bezterminowej, nielimitowanej licencji na dostarczone (wykonane) w ramach realizacji projektu oprogramowanie Systemu oraz przekazanie Zamawiającemu wszystkich zakupionych i wykorzystywanych w projekcie licencji.

**AD 17)**

Wykonawca musi przekazać Zamawiającemu potwierdzenia zakupu gwarancji producenta wraz ze wsparciem na okres 5 (pięciu) lat od daty podpisania Protokołu Końcowego. Gwarancje na serwery oraz macierze muszą uwzględniać zachowanie uszkodzonych dysków u Zamawiającego.

**AD 18)**

**Zadaniem Wykonawcy będzie nieodpłatne świadczenie usługi utrzymania całego Systemu przez okres 5 lat od daty podpisania Protokołu Końcowego Odbioru Prac.**

W ramach usługi utrzymania Wykonawca zobowiązany będzie do:

* + - ciągłego monitorowania funkcjonowania Systemu w trybie 24/7/365 wszystkich elementów Systemu poprzez zastosowanie dedykowanego oprogramowania (progi alarmowania zostaną ustalone na etapie projektowania)
		- okresowego (raz w miesiącu) przeglądu funkcjonowania Systemu
		- prowadzenie działań prewencyjnych mających na celu zapewnienie bezawaryjnej pracy Systemu
		- wydawania rekomendacji dotyczących przeprowadzenia zmian w konfiguracji, oprogramowaniu, sprzęcie w celu poprawienia funkcjonowania Systemu. Takie modernizacje uzgodnione z Zamawiającym muszą być wykonane na koszt Wykonawcy w ramach świadczenia usługi
		- bieżącego zarządzania (administrowania) Systemem tj. oprogramowaniem, bazami danych oraz innymi komponentami
		- bieżącego prowadzenia elektronicznej dokumentacji (dziennik systemowy) wszystkich działań związanych z utrzymaniem
		- aktualizacji oprogramowania w celu usunięcia stwierdzonych nieprawidłowości, dodania nowych funkcjonalności lub zastąpienia istniejącej wersji oprogramowania nowszą wersją, zgodnie z zasadami aktualizacji
		- aktualizacji systemów operacyjnych, oprogramowania gotowego oraz aktualizowanie i serwisowanie zakupionego sprzętu, przy czym aktualizacje oznaczone przez producenta jako krytyczne winny być zainstalowane nie później niż 24h od publikacji
		- realizacji działań naprawczych wynikających z analizy ujawnionych problemów, wykrytych błędów i wad systemów, niewłaściwego działania Systemu, spadku wydajności, itp.
		- obsługi zgłoszeń, otrzymanych od administratorów
		- przeprowadzania okresowych (raz w miesiącu) testów odtworzeniowych w oparciu o tworzone kopie zapasowe (weryfikacja poprawności odtworzenia danych z kopii zapasowej zgodnie z ustalonym wcześniej z Zamawiającym harmonogramem i zakresem)
		- asystowania i współpracowania z podmiotami świadczącymi usługi gwarancyjne
		- raz w miesiącu przesyłania do Zamawiającego raportu z wykonanych czynności w ramach usługi utrzymania

**Serwer logów**

Zadaniem Wykonawcy będzie utworzenie u Zamawiającego serwera logów odpowiedzialnego za zbieranie logów w postaci zdarzeń z aplikacji, systemów operacyjnych serwerów wchodzących w skład rozwiązania, firewalli, load balancerów, itp. Dostęp do logów zapewni interfejs graficzny, umożliwiający filtrowanie, analizę logów.

W celu zapewnienia rozliczalności, operacje użytkowników oraz obiektów systemowych wykonywane z uprawnieniami administracyjnymi, w tym operacje dotyczące zmiany konfiguracji zabezpieczeń lub przetwarzania danych, powinny być odnotowywane w logach systemowych.

**Repozytorium Kodów Źródłowych**

Wykonawca będzie zobowiązany do prowadzenia Repozytorium Kodów Źródłowych w taki sposób, aby była dostępna każda kolejna wersja oraz pełna rejestracja zmian wprowadzonych do kodów źródłowych.

**Obsługa zgłoszeń**

W celu zapewnienia wysokiego poziomu obsługi zgłoszeń i napotkanych błędów w funkcjonowaniu Wykonawca powinien zapewnić 3 kanały komunikacyjne: za pośrednictwem Systemu Zgłoszeń, poczty elektronicznej i telefonicznie.

System Zgłoszeń powinien być dostępny tylko dla administratorów wojewódzkich i administratora generalnego. Do podstawowych zadań tego systemu powinno należeć: przyjmowanie, rejestrowanie oraz powiadamianie o przyjęciu zgłoszeń, obsługa zgłoszeń poprzez umożliwienie dokonywania kategoryzacji i priorytetyzacji, a następnie przydzielania osób do realizacji zgłoszeń, dokonywania zapisów z poszczególnych etapów realizacji zgłoszeń aż do ich zamknięcia. System musi umożliwiać przeglądanie zgłoszeń, wysyłanie powiadomień o etapach realizacji usługi, a także generowanie raportów ilości zgłoszeń i czasów ich obsługi.

**Błędy Systemu**

Zamawiający wymaga, aby dostępność Systemu (parametr SLA) wynosiła 99,8 % w skali każdego miesiąca(30 dni) 99,9 % (30 minut). Dostępność Systemu rozumiana jest jako czas działania bez błędów w stosunku do całości czasu w danym okresie.

W przypadku wystąpienia błędów Krytycznych Wykonawca Systemu zapewni przywrócenie działania Platformy - RTO (Recovery Time Objective) w ciągu maksymalnie: 15 minut

W przypadku wystąpienia błędów Krytycznych skutkujących utratą danych Wykonawca Systemu zapewni odtworzenie stanu Systemu wraz z danymi - RPO (Recovery Point Objective) według stanu maksymalnie: 30 minut

W razie otrzymania przez Wykonawcę Systemu zgłoszenia lub w razie uzyskania przez Wykonawcę Systemu wiedzy o wystąpieniu błędu z innego źródła niż Zgłoszenie (w tym we własnym zakresie), Wykonawca Systemu zobowiązuje się do niezwłocznego usunięcia takiego błędu.

**Zamawiający ustala 2 kategorie błędów: krytyczne i mniejszej wagi**

**Błąd krytyczny** rozumie się w szczególności sytuację, w której nie jest możliwe prawidłowe użytkowanie Systemu z powodu uszkodzenia lub utraty spójności danych, struktur danych, błędnego funkcjonowania platformy systemowo-sprzętowej lub innej przyczyny powodującej, że system nie działa zgodnie z wymaganiem zamówienia. Jednocześnie nie jest znane obejście umożliwiające realizację celu zadania. Ponadto błędy krytyczne mają jedną lub więcej z poniższych cech:

1. Brak możliwości zalogowania się do Aplikacji Operacyjnej.
2. Brak możliwości zalogowania się do Aplikacji Treningowej.
3. Brak możliwości zalogowania się do Aplikacji OFFLINE.
4. Brak możliwości publikowania zdarzeń i informacji w Portalu Informacyjnym.
5. Nie funkcjonowanie Portalu Informacyjnego.
6. Awaria mechanizmu importu danych z systemów zewnętrznych.
7. Awaria modułu komunikacyjnego (brak możliwości ostrzegania, alarmowania i informowania, dystrybuowania ostrzeżeń, alarmów i informacji w systemie)
8. Brak możliwości pracy 15 000 użytkowników jednocześnie.
9. Brak możliwości wykonywania operacji w systemie
10. Awaria mechanizmu exportu danych do systemów zewnętrznych.
11. Awaria wyświetlania map cyfrowych.
12. Awaria funkcjonalności sporządzania analiz przestrzennych.
13. Awaria funkcjonalności wyświetlania zdarzeń i informacji w systemie.
14. Awaria funkcjonalności administrowania użytkownikami.
15. Awaria funkcjonowania modułu sił i środków.
16. Awaria powiązania wprowadzanych zdarzeń z wyświetlaniem przypisanych użytkownikowi procedur postępowania.
17. Awaria wyświetlania danych kwerendy o dostępność łóżek na określonym obszarze.
18. Awaria funkcjonalności raportowania sytuacyjnego i doraźnego (sporządzania raportów ich przekazywania na kolejne szczeble scalające dane).
19. Samoczynne wylogowywanie z aktywnej sesji użytkowników więcej niż 1 raz na godzinę.
20. Wykazanie podatności (luk w systemie) przez podmiot CSIRT GOV itp.
21. Błędy związane z bezpieczeństwem przechowywania i przetwarzania danych, które mogą wpłynąć na: uwierzytelnianie, niezaprzeczalność, poufność, integralność, dostępność, rozliczalność.

**Błędy mniejszej wagi – wszystkie inne błędy, nie będące krytycznymi to jest w szczególności:** rozumie się niezgodne z dokumentacją użytkową lub wymaganiami Zamawiającego określonymi w niniejszym OPZ lub innych dokumentach wytworzonych w czasie wdrożenia, działanie oprogramowania Systemu lub działania innego oprogramowania (np. standardowego), w skutek, którego niezgodnie zadziałało oprogramowanie Systemu. Jednocześnie znane jest obejście umożliwiające realizację celu zadania. Ponadto błędy mniejszej wagi mają jedną lub więcej z poniższych cech:

1. Awaria funkcjonowania aplikacji OFFLINE.
2. Przekroczenie czasu dystrybucji wiadomości powyżej 5 min.
3. Brak sygnalizacji dźwiękowej i wizualnej o wprowadzonym zdarzeniu (otrzymanej informacji).
4. Awaria funkcjonalności sporządzania analiz przestrzennych z wykorzystaniem modułu chemicznego wg metodyki ERG.
5. Pozostawianie na mapie w miejscach wygaszonego zdarzenia symboli nie wygaszonego zdarzenia.
6. Nie wyświetlanie po kliknięciu na znak (symbol) zasobu opisu tego zasobu.
7. Brak możliwości podłączania i wyświetlenia WMS z geoportali gov.pl
8. Brak możliwości sterowania przejrzystością wyświetlanych warstw na mapie użytkownika.

W zależności od kategorii błędu Wykonawca winien gwarantować następujący czas realizacji Zgłoszeń

|  |  |  |
| --- | --- | --- |
| **Kategoria Błędu** | **Czas Reakcji** | **Czas Naprawy** |
| Krytyczny | 5 minut | 8 godzin |
| Mniejszej Wagi | 5 minut | 36 godzin |

Usunięcie błędu nie może prowadzić do naruszenia struktur i integralności danych, do utraty danych lub wpływać negatywnie na funkcjonowanie Systemu.

Jeżeli usunięcie błędu możliwe jest wyłącznie poprzez wprowadzenie zmian do Systemu, Wykonawca może wystąpić do Zamawiającego o zgodę na wydłużenie czasu naprawy, wprowadzając jednocześnie jej obejście. Wprowadzenie obejścia odbywa się w terminie odpowiednim dla kategorii błędu. Nowy termin naprawy powinien zostać ustalony wspólnie przez Strony biorąc pod uwagę zakres koniecznych zmian.

Zastosowanie obejścia nie zwalnia Wykonawcy Systemu z obowiązku naprawy.

Czas naprawy uznaje się za dotrzymany, jeżeli przed jego upływem błąd zostanie usunięty lub zostanie zastosowane obejście celem uzyskania rezultatu tożsamego z usunięciem błędu lub czasowym wykluczeniem występowania błędu.

Widok kooperacji systemu.



Aplikacja Operacyjna – 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;

Główne funkcjonalności systemu

**Moduł komunikacyjny:**

Głównym przeznaczeniem modułu jest zapewnienie szybkiej i niezawodnej komunikacji pomiędzy wszystkimi uczestnikami systemu. W tworzonym systemie cała wymiana informacji odbywa się w obrębie systemu, który musi umożliwić maksymalną możliwą skuteczność dostarczenia informacji do wszystkich adresatów.

Grupy kontaktów (ta funkcja musi umożliwiać proste tworzenie grup kontaktów przez każdego użytkownika dla jego potrzeb poprzez wybieranie instytucji (urzędu). System musi umożliwiać wykorzystanie utworzonych grup kontaktów do przesyłania informacji, ostrzeżeń i alarmów.

Administrator generalny powinien mieć możliwość tworzenia i udostępniania grup do wykorzystania przez użytkowników szczebla wojewódzkiego i centralnego (tzw. grupy globalne o dowolnie tworzonej nazwie 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,
* gminy województwo …. .

Książka Globalna (odzwierciedlająca strukturę hierarchiczną administracji umożliwia wyszukiwanie instytucji, osób, edycję ich danych ze względu na szczebel organizacyjny):

* + - Krajowy
		- Wojewódzki
		- Powiatowy
		- Gminny

W związku z tym system musi zapewniać:

1. Tworzenie i modyfikację globalnej książki adresowej użytkowników systemu zawierającej co najmniej:
* nazwa instytucji,
* imię i nazwisko,
* numer identyfikacyjny,
* funkcja (stanowisko służbowe),
* adres instytucji (podmiotu),
* adres e-mail\_1,
* adres e-mail\_2,
* numer telefonu\_1,
* numer telefonu\_2
* numer telefonu\_3
* nr FAX\_1 (do wykorzystania w funkcji wysyłania FAX)
* nr FAX\_2 (do wykorzystania w funkcji wysyłania FAX)
* numer tel. komórkowego\_1 (do wykorzystania w funkcji wysyłania SMS)
* numer tel. komórkowego\_2 (do wykorzystania w funkcji wysyłania SMS)

Powyższe operacje będą mogły być dokonywane jedynie przez uprawnionych użytkowników. System musi rejestrować kto i kiedy wprowadził (modyfikował) dane. System musi umożliwiać globalne potwierdzenie aktualności danych za użytkowników instytucji. W wyniku realizacji globalnego potwierdzenia aktualności system wstawia bieżącą datę – jako datę aktualizacji).

Użytkownikiem może być albo osoba (pracownik), albo instytucja (CZK, inspekcja, straż, służba), ZZR, ZDR itp.

W tym przypadku dane teleadresowe dotyczą zdefiniowanego stanowiska operacyjnego w danej jednostce;

* Definiowanie i modyfikowanie globalnych list adresatów (funkcjonalność dostępna dla administratorów szczebla wojewódzkiego i administratora generalnego oraz RCB;
* Definiowanie i modyfikowanie list adresatów poprzez wybór adresatów z globalnej książki adresowej. Każdy użytkownik systemu może utworzyć i modyfikować wiele utworzonych przez siebie list;
* Możliwość wysłania wiadomości do:
	+ wybranego adresata (adresatów)
	+ adresatów własnych grup
	+ wszystkich adresatów z listy, grup publicznych (tylko jeśli takie uprawnienie przydzielił administrator)
* Możliwość wybrania priorytetu wysyłanej wiadomości:
	+ wysoka
	+ normalna
	+ niska
* Możliwość żądania potwierdzenia zapoznania się z komunikatem. Przy wyborze takiego sposobu doręczenia komunikatu odbiorca ma możliwość potwierdzenia skuteczności dostarczenia wiadomości poprzez jej otwarcie i wprowadzenie swojego identyfikatora.
* Możliwość wysłania informacji na wybrany e-mail (grupę e-mail użytkowników) – zgodnie z przydzielonymi uprawnieniami jako:
	+ Informacja
	+ Ostrzeżenie
	+ Alarm
* Możliwość automatycznego przetworzenia informacji w systemie z edytowalnej na postać PDF i wysłania informacji na wybrany FAX (grupę / grupy FAX zdefiniowanych użytkowników systemu (odbiorców);
* Sygnalizację na stacji roboczej adresata, (wizualna i dźwiękowa), otrzymania komunikatu wymagającego potwierdzenia otrzymania. System powinien zapewnić automatyczne dotarcie potwierdzenia do nadawcy po otwarciu wiadomości przez adresata (w tym informacji o potwierdzeniu autoryzacji odczytu jeśli zaznaczono przy wysyłce taki obowiązek);
* Możliwość śledzenia przez nadawcę komunikatu skuteczności doręczenia wiadomości.

Użytkownicy pogrupowani są podmiotami (instytucjami) z uwzględnieniem statusu przy każdym użytkowniku (wysłano, odebrano, odebrano i potwierdzono).;

* Możliwość automatycznego lub ręcznego wysłania wiadomości SMS do odbiorców, którzy nie potwierdzili odbioru komunikatu. Możliwość wysłania takiej wiadomości do wszystkich adresatów z listy z treścią z linijki tematu;
* Komunikaty w systemie muszą być opatrzone unikalnym identyfikatorem. Administrator wojewódzki musi posiadać możliwość odczytu ilości wysłanych (otrzymanych) komunikatów, ostrzeżeń, alarmów i wiadomości (za swoje województwo) - za m-c, kwartał i rok.
* Wszystkie komunikaty o określonym priorytecie muszą być zapisywane w bazie danych. Informacja powinna zawierać co najmniej identyfikator komunikatu, jego treść, identyfikator nadawcy, priorytet komunikatu oraz datę i czas emisji;
* W bazie danych muszą być także rejestrowane wszystkie czynności związane z wysyłaniem i odbiorem komunikatów o określonym priorytecie. Informacja ta musi być sygnowana znacznikiem czasu i musi zawierać co najmniej identyfikator komunikatu, identyfikator nadawcy lub odbiorcy oraz rodzaj czynności;
* Możliwość wygenerowania raportu z chronologią procesu przekazania wybranych komunikatów;
* System musi umożliwiać automatyczne wstawianie do raportów z dyżurów następujących treści otrzymanych informacji, zdarzeń, alarmów ostrzeżeń i wszystkich wysyłanych (wprowadzanych do systemu) informacji, alarmów ostrzeżeń i zdarzeń.
* System ma za każdym razem pytać użytkownika, czy wstawić tą treść do raportu.
* informacje wchodzące powinny min. zawierać: treść informacji, data i godz. wysłania, nadawca, instytucja (podmiot), priorytet informacji. Przy każdej informacji po jej odczytaniu powinna być możliwość jej przesłania dalej do globalnych lub własnych grup adresatów;
* informacje wychodzące (treść informacji, data i godz. wysłania, nadawca, instytucja (podmiot), priorytet informacji, godz. przyjęcia, przyjmujący, nazwa instytucji przyjmującego, godz. odczytania). Użytkownik powinien mieć możliwość zdefiniowania i zapisania w swoim profilu treści własnej stopki którą będzie mógł dodawać do wysyłanych dokumentów.
* Funkcjonalność wysyłania informacji musi umożliwiać wygenerowanie pliku dla użytkownika w postaci EXCEL lub PDF wykazu wysłanych, doręczonych i niedoręczonych informacji) z następującymi danymi:
	+ Nazwa instytucji
	+ Nazwa użytkownika
	+ Treść informacji
	+ Status informacji
		- Wysłana
		- Data i godzina wysłania
			* Sposób wysłania
				+ Aplikacja
				+ FAX
				+ E-mail
				+ SMS
		- Odebrana (dotyczy wyłącznie informacji wysłanych w systemie nie na zewnątrz systemu)
			* (data godz.)
		- Odebrana i potwierdzona (data godz.) (dotyczy wyłącznie informacji wysłanych w systemie nie na zewnątrz systemu)

Z systemu ST CPR do „Systemu Wczesnego Ostrzegania, Alarmowania i Informowania 2.0” – wszystkie przekazywane zgłoszenia wpływają jako informacje, których adresatami są:

- RCB

- WCZK – właściwe dla CPR przekazującego informację.

- inne podmioty (administrator generalny systemu musi posiadać możliwość wprowadzenia kolejnych podmiotów do listy otrzymujących informację z ST CPR. Schemat informacji z systemu STCPR – zgodny z formatką tego systemu.

**Alert RCB** (funkcja musi umożliwiać w przygotowanym predefiniowanym formularzu sformułowanie wniosku do Dyrektora RCB o uruchomienie Alertu RCB na określonym obszarze: **powiatu (powiatów, miasta n.p.p.), województwa**. Wszystkie województwa i powiaty muszą być powiązane z kodem TERYT.

**WCZK** (funkcjonalności dla WCZK)

* **Utwórz** /modyfikuj projekt  (Obszary do objęcia alertem muszą być wybierane ze słownika poprzez zaznaczenie checkbox powiatu)
	+ Akceptacja wnioskodawcy
	+ Wyślij do RCB
	+ Archiwum wysłanych wniosków w tym:
		- status odczytania przez RCB,
		- status uruchomienia/ odmowy RCB
		- status wysłania wniosku przez RCB do operatorów
		- wyszukiwanie poprzez wskazanie okresu dat od – do,
		- filtrowanie,
		- czyszczenie filtra,
		- możliwość wyeksportowania wniosku w standardzie WORD i PDF) – na podpis Wojewody (osoby upoważnionej przez Wojewodę)

**RCB** (funkcjonalności dla RCB)

* + - potwierdzenie otrzymania wniosku z WCZK, (z chwilą odczytania informacji przez RCB, w WCZK przy wysłanym alercie automatycznie pojawi się informacja potwierdzająca odczytanie wysłanego wniosku);
		- potwierdzenie uruchomienia wniosku / odmowa uruchomienia/ (z chwilą potwierdzenia uruchomienia / odmowy przez  RCB w WCZK przy wysłanym alercie automatycznie  pojawi się informacja o statusie;
		- modyfikuj (modyfikacja treści dla operatorów telekomunikacyjnych w predefiniowanym dla RCB formularzu oraz wyeksportowanie treści do pliku edytowalnego WORD – jako wariant pominięcia dalszych kroków)
		- akceptacja RCB
		- wyślij do operatora (umożliwia wysłanie wniosków w predefiniowanych dla RCB formularzach do operatorów telefonii komórkowej (E-mail, FAX) oraz automatycznie zapisuje informację do raportu z dyżuru umożliwiając edycję zapisanych treści
		- archiwum wysłanych wniosków do operatorów telekomunikacyjnych - funkcjonalność musi umożliwiać:
			* wyszukiwanie poprzez wskazanie okresu dat od – do,
			* filtrowanie,
			* zliczanie alertów za zadany okres
			* czyszczenie filtra,
			* wyeksportowanie formularzy do standardu edytowalnego WORD oraz PDF)
* **Skrzynka odbiorcza** – musi przechowywać wszystkie otrzymane w systemie informacje
	+ Wiadomości (wiadomości odczytane)
	+ Nowe wiadomości (wiadomości do odczytania)
	+ Ostrzeżenia (ostrzeżenia odczytane)
	+ Nowe ostrzeżenia (ostrzeżenia do odczytania)
	+ Alarmy (alarmy odczytane)
	+ Nowe alarmy (alarmy do odczytania)
* **Wysłane wiadomości**
	+ Zestawienie wysłanych informacji ze statusem:
		- wysłane
		- odczytane
		- odczytane i potwierdzone
* **Kontakty** (wyświetla dla użytkownika wyłącznie kontakty zgodnie z przydzielonymi uprawnieniami):
	+ dla użytkowników systemu szczebla centralnego (ministerstwa, RCB, WCZK) widoczne są wszystkie kontakty z podziałem administracyjnym)
	+ dla użytkowników systemu szczebla służb i straży wojewódzkich widoczne są kontakty z podziałem administracyjnym od szczebla wojewódzkiego do gminy włącznie;
	+ dla użytkowników systemu szczebla powiatowego widoczne są kontakty z podziałem administracyjnym od szczebla wojewódzkiego do gminy włącznie;
	+ dla użytkowników systemu szczebla gminnego widoczne są kontakty z podziałem administracyjnym od szczebla wojewódzkiego do gminy włącznie;
* Funkcja „Mój profil” (wyświetla dane profilu użytkownika umożliwiając ich aktualizację w zakresie telefonów, fax, e-mail)
* Funkcja „Komunikaty systemowe” (umożliwia śledzenie każdemu użytkownikowi stanu powiadamiania instytucji o wprowadzonym do systemu zdarzeniu)
* Funkcja „Władze” (umożliwia wprowadzenie i aktualizację informacji dotyczącej kierowniczej kadry poszczególnych szczebli administracji, służb inspekcji i straży. Szczebel krajowy jest widoczny wyłącznie dla podmiotów szczebla krajowego i WCZK. Osobę do zakładki władze wybiera się z danych kontaktowych przypisując jej funkcję, oraz pozycję na liście władz. W danych „Władze” przy osobie powinny się wyświetlać min. następujące informacje: Instytucja (podmiot) funkcja, imię i nazwisko, tel. kom., tel, stacj., e-mail, FAX)
* W systemie występują następujące szczeble organizacyjne:
	+ Krajowy (ministerstwa, RCB, instytucje centrale, komendy główne służb i straży, inspekcje szczebla krajowego, szpitale resortowe)
	+ Wojewódzki (UW, służby inspekcje i straże wojewódzkie, szpitale wojewódzkie, resortowe)
	+ Powiatowy (SP, UM n.p.p., służby inspekcje i straże powiatowe, szpitale powiatowe)
	+ Gminny (UG, UM, UMiG, ZDR, ZZR)
		- Sołectwa (sołtys)
* Archiwum wysłanych FAX
* Archiwum wysłanych SMS
* Archiwum wysłanych e-mail

**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 (w oparciu o zdefiniowany katalog zagrożeń wynikający z WPZK (KPZK);
* Dodaj zdarzenie ZDR (uproszczone wprowadzanie zdarzeń przez użytkownika systemu z zakładu dużego ryzyka wystąpienia poważnej awarii przemysłowej. Dla tego trybu system automatycznie pobiera przypisaną lokalizację zakładu z którego jest użytkownik systemu. Użytkownik musi wyłącznie wprowadzić krótką informację dot. tego co się wydarzyło lub predefiniowaną wcześniej treść słownikową np.:
	+ Uwolnienie substancji niebezpiecznej
	+ Pożar
	+ Wybuch

Tryb rozprowadzania informacji o zdarzeniu w ZDR – jak dla innych zdarzeń. Administrator musi mieć możliwość edycji (uzupełniania) słowników.

* Dodaj zdarzenie bez alarmu - np. zdarzenie historyczne nie bieżące które nie wymaga natychmiastowego działania – tylko dokumentuje jego wystąpienie (w oparciu o zdefiniowany katalog zagrożeń wynikający z KPZK (WPZK). Wprowadzenie tego zdarzenia nie powoduje emisji dźwiękowego powiadamiania – tylko poprzez sygnalizację migającej ikony alarmu.
* 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). Funkcjonalność musi umożliwiać wysłanie informacji do zdefiniowanych grup globalnych lub grup użytkownika, pojedynczego użytkownika.
* MGCO
	+ Dodaj meldunek (meldunek jak Międzynarodowa Głowna Centrala Ostrzegawczo – Alarmowa dla Odry). Funkcjonalność dostępna wyłącznie dla województw:
	+ Dolnośląskiego
	+ Opolskiego
	+ Śląskiego
	+ Lubuskiego
	+ Zachodniopomorskiego

oraz MKOO Wrocław (Międzynarodowej Komisji Ochrony Odry przed zanieczyszczeniami). Wysyłany meldunek będzie wg jednolitego wzoru – zgodnie ze schematem alarmowania zawartym w „Planie Ostrzegawczo – Alarmowym dla Odry”.

* Meldunki MGCO

W odniesieniu do działania MGCO państwa członkowskie Czechy i Niemcy otrzymują meldunek wygenerowany z systemu w postaci e-mail i FAX. System powinien umożliwiać późniejsze włączenie MGCO Niemiec i Czech do systemu oraz przypisanie im schematów rozsyłania meldunków do Polski i Czech.

Musi istnieć możliwość rozszerzenia ilości podmiotów raportujących, wprowadzania dodatkowych schematów alarmowania dla włączanych podmiotów raportujących i wskazania schematu rozsyłania wprowadzanego meldunku. System musi umożliwiać zawężenie wyświetlanych modułów do MGCO (musi istnieć możliwość udostępnienia tej funkcjonalności do wyłącznego wglądu i użytkowania przez WCZK i inne podmioty).

* + Wszystkie zdarzenia - wyświetla wszystkie zdarzenia bieżące. Przy każdym zdarzeniu 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 za zadany okres (pojedynczego zdarzenia) z geolokalizacją i opisem na mapie cyfrowej )
* 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 i stanowisko 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)

W raporcie z dyżuru dla danej instytucji (CZK) powinna być możliwość zapisu wszystkich otrzymanych i wysłanych informacji i ostrzeżeń z możliwością edycji, usunięcia treści.

* 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/ oraz do wyświetlenia obszarów objętych ostrzeganiem na mapie
	+ 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 jako warstwa do wyświetlenia na mapie
	+ Wodowskazy - z hydromonitora – jako warstwa do wyświetlenia na mapie
	+ Wizualizacja siły i kierunku wiatru - jako warstwa do wyświetlenia na mapie
* Utrudnienia drogowe (Przekazywane do systemu w standardzie XML z możliwością geolokalizowania ich na mapie cyfrowej włączane i wyłączane na żądanie jako warstwa).
* Informacja z PGW Wody Polskie / RZGW (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.

 **Meldunki „do systemu” SI Promień**

Funkcjonalność musi umożliwiać sporządzenie i wysłanie meldunku zgodnego z metodyką ATP-45D w standardzie ADATP3.

System musi umożliwiać min.:

* + - pobranie współrzędnych zdarzenia (z już wprowadzonego meldunku o zdarzeniu)
		- pobranie współrzędnych zdarzenia poprzez wskazanie miejsca na mapie,
		- wybieranie adresu (województwo, powiat, gmina, miejscowość, ulica, nr budynku)
		- podanie współrzędnych GPS;
		- wstawienie danych dotyczących informacji o środkach przenoszenia i ich ilości
		- informacji o uwolnionych środkach CBRN
* charakterystyce warunków terenowych i szacie roślinnej
* wysłanie meldunku w standardzie AdatP3 do CD KSWSiA

 **Meldunki „z systemu” SI Promień**

* + Wysłane
	+ Odebrane

 Przechowuje wszystkie meldunki z podziałem na wysłane i odebrane. Klikniecie na meldunek lub zaznaczenie checkbox przy meldunku umożliwia zwizualizowane pojedynczego zobrazowania, wielu wybranych zobrazowań i wszystkich, dla obszaru województwa, województw i kraju;

* przyjęcie meldunku z CD KSWSiA w postaci prognozy musi umożliwiać jego publikację dla użytkowników systemu i w PI. (O publikacji meldunku w PI decyduje WCZK, RCB);

 Meldunek prognozy z systemu SI Promień wchodzi do systemu poprzez moduł komunikacyjny i podlega przekazaniu – zgodnie ze schematem informowania ostrzegania – jak w odniesieniu do zdarzeń. (UWAGA – dodatkowo informacja jest przekazywana do pozostałych podmiotów wyszczególnionych w Krajowym Planie Współdziałania).

* Informacja z systemu ruchu pociągów (lokalizacja pociągu na mapie, rodzaj składu pasażerski/towarowy, nr pociągu)

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

Odbiorcami docelowymi są:

* + - wszyscy użytkownicy systemu szczebla gminnego na terenie którego doszło do zdarzenia oraz gmin sąsiadujących danego województwa;
		- wszyscy użytkownicy systemu szczebla powiatowego na obszarze którego wprowadzono zdarzenie;
		- wszyscy użytkownicy systemu 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, które może przekazać inf. dot. tego zdarzenia do wybranego PCZK na swoim obszarze odpowiedzialności;
		- **Użytkownicy szczebla centralnego (krajowego) w tym RCB otrzymują każdą informację o zdarzeniu. Zaznaczona w ten sposób informacja o zdarzeniu Dyżurnemu RCB sygnalizuje się w ten sam sposób jak dla przyjętej automatycznej procedury (dźwiękowo i wizualnie). Administrator generalny musi posiadać możliwość edycji tej procedury.**

Użytkownik który wprowadził zdarzenie, i szczeble nadrzędne muszą posiadać możliwość uzupełniania informacji o zdarzeniu, podejmowanych działaniach, zaangażowanych siłach i środków. 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 do innego województwa (województw).

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 dostępne wyłącznie dla WCZK i RCB. 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, kraj)
		- Archiwum zdarzeń (katalog w którym przechowywane są wszystkie informacje o zdarzeniach przeniesionych do archiwum z możliwością przywrócenia ich statusu do aktywnych)
		- 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 Portalu Informacyjnym;
		- w RSO (Regionalnym Systemu Ostrzegania);
	+ tworzenie doraźnych zestawień informacji za dowolny okres z wprowadzonych do systemu zdarzeń i informacji;
	+ zaimplementowane obowiązujące „Zasady postępowania ratowniczego” na podstawie ERG umożliwią 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 lub dane wpisywane ręcznie przez użytkownika;
	+ 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 i treningów;
	+ 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) 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 min. niżej wyszczególnione funkcjonalności dostępne dla każdego użytkownika.

* wprowadzanie nowych zasobów poprzez wskazanie miejsca na mapie, selekcję podziału administracyjnego lub podanie współrzędnych geograficznych;
* wyszukiwanie zasobów
	+ wg kryterium wpisanego przez użytkownika np. część nazwy zasobu;
	+ wg kryterium selekcji obszaru (użytkownik wybiera ze słownika predefiniowany obszar np. województwa, kilka powiatów, powiat, kilka gmin, gmina)
	+ poprzez selekcję kategoriami i podkategoriami zasobów;

Uruchomienie wyszukiwania wyświetla na mapie położone wyszukiwanego zasobu, a po kliknięciu w poszczególne ikonki zasobu wyświetlają się wszystkie wprowadzone informacje o danym zasobie. Opcja wyszukiwania musi umożliwiać wyeksportowanie danych uzyskanych kwerendą do tabeli EXCEL lub PDF.

Baza sił i środków powinna zawierać poniższy podział zasobów:

* + 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
	+ jednostki wojskowe
	+ 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

Powyższy podział może być zmodyfikowany przez wykonawcę po uzyskaniu zgody Zamawiającego (np. w wypadku potrzeby dostosowania do wykorzystania innych struktur baz danych w tym w szczególności aplikacji OFFLINE).

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 administratorzy wojewódzcy. Będzie on dostępny wyłącznie dla użytkownika któremu przydzielono taki dostęp i który zainstalował aplikację OFFLINE na swoim komputerze lokalnym.

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 musi wyświetlić w zestawieniu oraz na mapie zasoby w województwie.
* Zapytanie o zasób w wybranych województwach i kraju musi wyświetlić w zestawieniu oraz na mapie zasoby tych wybranych województw lub całego kraju.

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
* zagrożenia epidemiologiczne
* zagrożenia epizootyczne
* zagrożenia fitosanitarne
* zagrożenia powodziowe
* zagrożenia pożarowe
* zagrożenia 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 km 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
* metoda wybrania określonej drogi (w całości lub odcinka drogi)

**Moduł obsługi mapy**

* Zmień serwis mapowy
	+ BDOT GUGIK
	+ Ortofotomapa GUGIK
	+ BDOT /z serwera GIS systemu/
	+ Ortofotomapa /z serwera GIS systemu/
	+ OpenStreetMap (Polska i świat) /z serwera GIS systemu/
* Skalowanie mapy min. 20 poziomów od skali 1:2000 /z serwera GIS systemu/
* 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 GUGiK 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 i alertach

**Moduł Raportowania**

* **Raport z dyżuru** (dla podmiotów pełniących dyżury)
	+ szczebel gminny
	+ szczebel powiatowy
	+ szczebel wojewódzki
	+ szczebel centralny

System musi samodzielnie tworzyć pełny raport automatyczny wstawiając wszystkie wpływające i wysyłane informacje, alarmy i ostrzeżenia. Użytkownik musi mieć możliwość samodzielnego tworzenia własnego raportu.

System musi przechowywać i umożliwiać wyeksportowanie raportów tworzonych automatycznie i raportów z dyżuru wg układu treści użytkownika.

* **raport doraźny**
	+ szczebel gminny (możliwość wyłączenia z raportowania)
	+ szczebel powiatowy
	+ szczebel wojewódzki
	+ szczebel centralny
* **raport dobowy**
	+ szczebel gminny (możliwość wyłączenia z raportowania)
	+ szczebel powiatowy
	+ szczebel wojewódzki
	+ szczebel centralny
* **raport sytuacyjny –** wg zadanego formatu raportowania
	+ szczebel gminny (możliwość wyłączenia z raportowania)
	+ 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

**Układ raportu doraźnego** (formularz raportu zgodny z obowiązującym w CAR)

I. Kategoria – rodzaj zdarzenia lub zagrożenia (z katalogu zdarzeń)

II. Przebieg (opis) zdarzenia/zagrożenia

Opis sytuacji, w tym przyczyny oraz czas i miejsce lub obszar (województwo, powiat, gmina, miejscowość) jego wystąpienia. Faktyczne i potencjalne skutki zdarzenia lub zagrożenia, w tym (o ile jest to możliwe do oszacowania): liczbę poszkodowanych (zabitych i rannych), liczbę zagrożonych osób (w tym zagrożonych lub objętych ewakuacją), liczbę zagrożonych lub uszkodzonych budynków (mieszkalnych i gospodarczych) i obiektów użyteczności publicznej (szkoły, szpitale itp.) oraz systemów infrastruktury krytycznej, a także opis innych potencjalnych skutków zagrożenia bezpośrednio związanych z zakresem działania raportującego podmiotu.

III. Przyczyna zdarzenia

IV. Podjęte i zamierzone działania. Opis sił i środków zaangażowanych i przewidywanych do uruchomienia.

V. Przewidywany rozwój wydarzeń – ocena i prognoza rozwoju sytuacji

VI. Wnioski i rekomendację (uwagi)

VII. Źródło informacji

**Układ raportu dobowego.** (formularz raportu zgodny z obowiązującym w CAR)

• tryb przekazywania raportu obecnie obowiązujący PCZK do WCZK (dyżurny WCZK sporządza i akceptuje treść raportu i przekazuje go do RCB raz na dobę,

• możliwość tworzenia raportu dobowego RCB na podstawie raportów z WCZK;

• podgląd raportów przez wszystkich użytkowników.

**Układ raportu sytuacyjnego. (**formularz raportu zgodny z obowiązującym w CAR)

**Raport inicjujący 1/2**

I. Opis i miejsce sytuacji, przyczyny zdarzenia, przebieg zdarzenia/zagrożenia

II. Trudności w dotarciu do miejsca zdarzenia

III. Podjęte i zamierzone działania, użyte siły i środki

IV. Czy siły i środki są wystarczające?

V. Czy planowane jest posiedzenie Zespołu Zarządzania Kryzysowego

VI. Ocena i prognoza rozwoju sytuacji, wnioski, rekomendacje, uwagi

VII. Alarmy przeciwpowodziowe (gminy i powiaty)

VIII. Pogotowia przeciwpowodziowe (gminy i powiaty)

IX. Inne zagrożenia, wprowadzane alarmy w zależności od potrzeb (np. pożary lasów, choroby zakaźne zwierząt, zanieczyszczenie powietrza)

**Raport inicjujący 2/2**

I. Zabici

II. Zaginieni

III. Ranni

IV. Ewakuowani

V. Uszkodzone budynki mieszkalne (szt.)

VI. Uszkodzone budynki gospodarcze (szt.)

VII. Obiekty oświatowe (szt.)

VIII. Obiekty służby zdrowia (szt.)

IX. Inne istotne obiekty (szt.)

X. Drogi (km)

XI. Mosty (szt.)

XII. Padłe i poddane ubojowi zwierzęta hodowlane (szt.)

XIII. Straty w uprawach (ha)

XIV. Wysokość szacowanych strat na terenie jednostki (zł)

XV. Zapomogi wypłacone przez gminy (zł)

XVI. Środki przekazane jednostce z budżetu państwa (zł)

XVII. Gospodarstwa, którym udzielono pomocy rzeczowej (szt.)

XVIII. Inne skutki zagrożenia

**Tryb raportowania uruchamiany przez jednostkę nadrzędną.**

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

**Generator formularzy raportowania**

Moduł ten jest miejscem przechowywania obowiązujących globalnych szablonów raportów.

Odpowiada za scentralizowane tworzenie nowych formularzy raportowania:

* 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  obsługi zdarzeń chemicznych** – zgodny z „Zasadami postępowania ratowniczego ERG”

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

**Moduł administracyjny**

* Komponent administracyjny musi umożliwiać administrowanie użytkownikami i podmiotami wraz z możliwością przeglądania listy podmiotów, użytkowników oraz
* dodawania, edytowania, kasowania, blokady konta, zmiany hasła konta, powiązania użytkownika z podmiotem, itp.
* Podczas dodawania konta użytkownika musi pojawić się kreator w którym można wpisać Imię i Nazwisko oraz wybrać z listy instytucję w której pracuje i określić aplikację do której będzie miał dostęp (operacyjna, treningowa, testowa, portal informacyjny). Login będzie generowany automatycznie według wytycznych Zamawiającego. Hasło dla użytkownika będzie generowane automatycznie zgodnie z politykami ustawionymi przez administratora generalnego. Po utworzeniu użytkownika powinna pokazać się wersja do wydrukowania ze wszystkimi danymi. System powinien posiadać zbiór wygenerowanych formularzy użytkowników. Administrator zakładając konto użytkownika obowiązkowo powinien zaznaczać checbox posiadania formularza zgody na przetwarzanie danych osobowych użytkownika. Bez zaznaczenia tego pola formularz nie powinien pozwolić na realizację kolejnych kroków.
* Administrator generalny, administratorzy wojewódzcy muszą mieć możliwość (tworząc konto użytkownika lub je modyfikując) określać zdefiniowaną rolę np.: 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.
* Lista użytkowników (z możliwością blokady konta, dodawania, edytowania i kasowania oraz ustawienia wybranego konta w tryb zapobiegania blokowaniu się). Opcja ustawiania zapobiegania blokowaniu konta musi rejestrować nazwisko administratora, który zaznaczył tą funkcjonalność dla konta użytkownika, IP komputera, datę i godz.
* lista użytkowników zalogowanych (musi umożliwiać wyświetlanie aktualnie zalogowanych użytkowników z następującą informacją: (imię i nazwisko, nazwa instytucji, województwo, powiat, 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, województwo, powiat, 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, województwo, powiat, 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 (przeglądanie, Gmina / GCZK, PCZK, służba (inspekcja) powiat, służba (inspekcja) województwo szpital, ZRM, WKRM, WCZK, RCB, ministerstwo, służba (inspekcja) kraj, administrator wojewódzki, administrator generalny itp. z zastrzeżeniem, że administrator wojewódzki nie może nadawać uprawnień ponad wojewódzkich i zastrzeżonych dla administratora generalnego.
* Globalna aktualizacja bazy danych sił i środków ze zbiorów plików (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 oraz pobranie danych z „Systemu Ostrzegania Alarmowania i Informowania Województwa Dolnośląskiego.

Funkcjonalność dostępna wyłącznie dla generalnego administratora systemu DUW.

* + Walidacja
	+ Wczytaj zbiór

System musi zachowywać informację dotyczącą osoby wczytującej zbiór (identyfikator oraz IP komputera) z którego wysłano dane do aktualizacji.

System musi posiadać mechanizm automatycznego skanowania plików pod kątem ich potencjalnego zainfekowania wirusem przed zaimportowaniem pliku.

* 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 – informacje o przeprowadzonych aktualizacjach (data, godz. aktualizacji, obszar objęty aktualizacją (np. województwo/województwa, kraj), nawa administratora, IP komputera z którego dokonano 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

Użytkownik może zmienić swoje hasło dopiero po zalogowaniu się do systemu, dodatkowo podając stare hasło.

**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,
* planowanie czynności doraźnych wynikających z toku pełnienia dyżuru oraz innych czynności bieżących;
* zaplanowanie realizacji zadań z półtorarocznym wyprzedzeniem w stosunku do bieżącej daty;
* moduł musi działać na zasadzie **“żółtej karteczki”;**
* położenie checkbox modułu 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 – umożliwia 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
	+ COVID-19 ( wyświetlanie danych dotyczących zakażeń i dostępności dedykowanej bazy łóżkowej z systemu COVID-19 RCB)

**Moduł Szpital**

* Złóż raport (funkcjonalność dostępna wyłącznie dla województwa dolnośląskiego)
* Przeglądaj raporty
* Archiwum raportów
* Dane szpitala
* Możliwości jednostki
* Oddziały
* Siły i środki
* Telefony
* Pracownie
* Wyposażenie
* Wyszukiwanie wolnych łóżek (funkcjonalność dostępna dla wszystkich użytkowników którym udostępniony zostanie ten moduł)
	+ W województwie
	+ W wybranych województwach
	+ W kraju

**Moduł Pogotowie Ratunkowe**

* 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.

Aplikacja treningowa

Posiada te same funkcjonalności co Aplikacja Operacyjna z wyłączeniem:

* Publikacji na Portalu Informacyjnym
* Publikacji w RSO
* Wysyłania SMS
* Wysyłania FAX
* Nie umożliwia raportowania o dostępnej bazie łóżkowej (ale umożliwia 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 dostępny 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 być połączona z aplikacją treningową SI PROMIEŃ.

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

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

Portal Informacyjny – musi być dostosowany do dostępu dla osób niedowidzących, tj. zgodność z wymogami WCAG 2.1 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, uwzględniając czasokres 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.

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.

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 |
| PGW WP RZGW | Państwowe Gospodarstwo Wodne Wody Polskie - Regionalny Zarząd Gospodarki Wodnej  |
| 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 |
| 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 |
| WAF | Web Application Firewall to transparentny system ochrony aplikacji webowych, tj. stron internetowych. |
| 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 |