Załącznik nr 5 do SWZ

Załącznik nr 1 do Umowy

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

„Budowa Modułu Telerehabilitacji z algorytmami sztucznej inteligencji w ramach Regionalnego Repozytorium Elektronicznej Dokumentacji Medycznej”

Projekt współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

Spis treści

1. Definicje i skróty

Użyte w niniejszym Opisie Przedmiotu Zamówienia (OPZ), Umowie i załącznikach wszelkie nazwy własne, normy, aprobaty, specyfikacje techniczne, systemy referencji technicznych, procesy charakteryzujące produkt lub usługę, należy rozumieć każdorazowo jak opatrzone dopiskiem „lub równoważne".

Definicja / skrót	Opis
Administrator Systemu / Modułu	Osoba (zespół osób) zajmująca się zarządzaniem Systemem / Modułem i odpowiadająca za jego sprawne działanie, posiadająca uprawnienia do części administracyjnych Systemu / Modułu.
Architektura Referencyjna	Zbiór zasad, wytycznych i standardów przeznaczony dla dostawców / producentów urządzeń do telerehabilitacji monitorujących i diagnozujących.
Backup	System kopii zapasowy danych cyfrowych.
Baza danych	Część architektury Systemu, program komputerowy pozwalający na gromadzenie i zarządzanie zbiorem danych lub jakichkolwiek innych materiałów i elementów zgromadzonych według określonej systematyki lub metody.
Błąd	Nieprawidłowe działanie Modułu, niezależnie od przyczyny takiej nieprawidłowości. W szczególności Błędem jest działanie Modułu niezgodnie z Dokumentacją. Błędom przypisane są kategorie.
Błąd Krytyczny	Nieprawidłowe działanie Modułu powodujące albo całkowity brak możliwości korzystania z Modułu albo takie ograniczenie możliwości korzystania z niego, że przestaje ono spełniać swoje podstawowe funkcje.
Błąd Poważny	Nieprawidłowe działanie Modułu powodujące ograniczenie korzystania z Modułu przy zachowaniu spełniania przez Moduł jego podstawowych funkcji.
Błąd Niskiej Kategorii	Nieprawidłowe działanie Modułu niepowodujące ograniczenia korzystania z Modułu. Przykładem Błędu Niskiej Kategorii jest np. błąd językowy w interfejsie.
Centrum Monitoringu	Miejsce, w którym ratownicy medyczni / personel medyczny pełnią stały dyżur w celu podjęcia odpowiednich działań w przypadku Zdarzenia oraz monitorują stan pacjenta.
CPD	Centrum Przetwarzania Danych.
Dokumentacja	Wszelka dokumentacja dotycząca Systemu, która jest dostarczana lub powstanie w ramach realizacji zamówienia m. in. instrukcja obsługi, Architektury Referencyjnej, dokumentacja powykonawcza.
HA	(High Availability) - określenie systemu informatycznego o wysokiej niezawodności i dostępności na poziomie nie mniejszym niż SLA 99,99% czasu w skali roku.
Karta użytkownika / Karta pacjenta	Zestawienie informacji o Pacjencie gromadzonych w celu realizacji telerehabilitacji, przekazane przez Użytkownika w formie papierowej.
Kod źródłowy	Wynik prac programistycznych pozwalający wyrazić w czytelnej formie strukturę oraz działanie Systemu.
SaaS	Oprogramowanie jako usługa (Software as a Service) to model udostępniania oprogramowania w chmurze, w którym dostawca chmury rozwija i utrzymuje aplikacje chmurowe, zapewnia ich automatyczne aktualizacje i udostępnia oprogramowanie swoim klientom za pośrednictwem Internetu.
Odbiór	Potwierdzenie przez Zamawiającego należytego wykonania Umowy. Dowodem dokonania Odbioru jest Protokół Odbioru Końcowego.
RREDM	Regionalne Repozytorium Elektronicznej Dokumentacji Medycznej budowane w ramach projektu „Budowa kujawsko-pomorskiego systemu udostępniania elektronicznej dokumentacji medycznej – I etap".
RTO	(Recovery Time Objective)- czas w jakim należy przywrócić procesy po wystąpieniu awarii.
RPO	(Recovery Point Objective)- akceptowalny poziom utraty danych wyrażony w czasie.
OPZ	Opis Przedmiotu Zamówienia.
Protokół Odbioru Końcowego	Dokument stanowiący potwierdzenie dokonania Odbioru w zakresie całości Umowy.

SLA	(Service Level Agreement) – wymogi w zakresie gwarantowanego poziomu świadczenia usług.
System / Moduł / Moduł Telerehabilitacji	System informatyczny, który będzie realizował zadania z zakresu telemedycyny i telerehabilitacji w ramach RREDM, opisany szczegółowo w niniejszej dokumentacji.
Użytkownik / Pacjent	Osoba objęta programem telerehabilitacji.
Zamawiający	Województwo Kujawsko-Pomorskie, Lider Projektu pn. „Budowa kujawsko-pomorskiego systemu udostępniania elektronicznej dokumentacji medycznej- I etap”.
Zdarzenie	Wywołanie przez Pacjenta lub samoczynnie przez Urządzenie, alarmu o zagrożeniu życia lub zdrowia Pacjenta.

2. Obowiązujące przepisy prawne

Zamawiający wymaga, aby przedmiot zamówienia był zgodny ze wskazanymi aktami prawnymi:

1. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. (Dz. U. z 2021 poz. 2070).
2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych, w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE z dnia 27.04.2016r. (Dz.U.UE.L.2016.119.1) RODO.
3. Ustawa z dnia 10.05.2018 r. o ochronie danych osobowych (Dz.U.2019.1781).
4. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U.2020.0.344).
5. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (Dz.U.2018.1544).
6. Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (tj. z 3.10.2018 r. Dz.U. z 2018 r.poz.2096).
7. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz.U.Nr.206 poz.1518).
8. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 159, poz. 948).
9. Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. Nr 128, poz. 1402, z późn. zm.).

3. Przedmiot zamówienia

1. Przedmiotem zamówienia jest „Budowa Modułu Telerehabilitacji z algorytmami sztucznej inteligencji w ramach Regionalnego Repozytorium Elektronicznej Dokumentacji Medycznej”, polegającego na:
   1) przygotowaniu projektu Modułu Telerehabilitacji,
   2) wytworzeniu oprogramowania, realizującego zadania telemedycyny i telerehabilitacji,
   3) wytworzeniu i wdrożeniu algorytmów sztucznej inteligencji do analizy danych spływających do Modułu Telerehabilitacji,
   4) przekazaniu Kodów źródłowych Systemu wraz z przeniesieniem autorskich praw majątkowych na Zamawiającego,
   5) zapewnienia dedykowanego środowiska teleinformatycznego HA w modelu chmury obliczeniowej wraz z backupem oraz pełną obsługą i utrzymaniem na potrzeby realizacji kompleksowej usługi,
   6) udostępnienie Modułu w modelu SaaS usługi opieki nad Pacjentem,
   7) realizacji kompleksowej usługi wraz z zapewnieniem niezbędnego oprogramowania, lub innych niezbędnych elementów składających się na jej prawidłowe funkcjonowanie,
   8) dostawie monitorującego sprzętu dostarczającego dane do Systemu,
   9) udzielenie nieodpłatnej gwarancji na cały przedmiot zamówienia.
2. Przedmiot zamówienia powinien zostać zrealizowany nie później niż do 31.10.2023 r.

4. Zakres zamówienia

1. W ramach zamówienia Wykonawca zaprojektuje, wykona, a następnie wdroży rozwiązanie, które w formie systemu informatycznego, będzie realizowało zadania Modułu Telerehabilitacji z algorytmami sztucznej inteligencji do analizy danych spływających do Systemu, opisane szczegółowo w niniejszym dokumencie. Celem realizacji przedmiotu zamówienia jest wsparcie w zakresie kreowania polityki zdrowotnej regionu z poziomu Lidera Projektu poprzez wprowadzenie funkcjonalności dotyczącej obszaru telemedycyny i telerehabilitacji w ramach Regionalnego Repozytorium Elektronicznej Dokumentacji Medycznej, która zostanie zrealizowana za pomocą Modułu Telerehabilitacyjnego i wzbogaci repozytorium o dodatkową funkcjonalność polegającą na udostępnieniu w modelu SaaS usługi opieki nad pacjentami, znajdującymi się w trakcie procesu rehabilitacji, przy założeniu, że cała dokumentacja powstała w wyniku działania Modułu będzie możliwa do zaimportowania do Regionalnym Repozytorium Danych Medycznych. W ramach zamówienia zostanie zrealizowany System do realizacji telemedycyny i telerehabilitacji. Zakupione zostanie kompletne rozwiązanie, w skład którego wchodzić będą między innymi oprogramowanie – platforma do realizacji funkcjonalności telerehabilitacji, która będzie umożliwiała zlecanie oraz nadzorowanie procesu rehabilitacji przez personel medyczny. Dodatkowo zostaną zakupione odpowiednie sensory monitorujące parametry biologiczne pacjentów.
2. Moduł Telerehabilitacji będzie składał się z następujących komponentów:
   1) Architektury Referencyjnej.
   2) Środowiska teleinformatycznego pozwalającego na świadczenie dostępu do Modułu Telerehabilitacyjnego w modelu SaaS.
   3) Procedury pozwalającej na uniwersalne zarządzanie Systemem.
   4) Rozwiązania składającego się z:
      a) Front Office – Interfejsu Użytkownika i personelu medycznego, dostępnego dla Użytkownika, członków rodzin, opiekunów, lekarzy, pielęgniarek i ratowników medycznych z interfejsem dostarczonym w polskiej wersji językowej umożliwiający:
         Dla Pacjenta:
         – gromadzenie wyników pomiarowych z urządzeń monitorujących telerehabilitację,
         – dostęp do wyników pomiarów,
         – dostęp do pomiarów dla wybranych członków rodziny / opiekunów,
         – monitoring Pacjentów przez członków rodzin / opiekunów.
         Dla lekarza / pielęgniarki:
         Plug – in do analizy (działanie lokalne):
         – analiza wyników pomiarów EKG wykonanych u Pacjenta w warunkach domowych,
         – analiza zdarzeń Pacjenta,
         – tworzenie raportów.
         Dla ratowników medycznych i pielęgniarek:
         – zarządzanie urządzeniami do telerehabilitacji i ich zdalną kontrolę,
         – dostęp do kartotek Pacjentów,
         – dostęp do bieżących zarejestrowanych pomiarów Pacjenta,
         – analiza zdarzeń Pacjenta,
         – wygodne opisywanie Zdarzeń,
         – zdalny nadzór nad Pacjentem,
         – personalizacja zakresów alarmowych,
         – raportowanie.
      b) Back Office – Interfejsu Administratora, dostępnego dla Administratora Systemu przez przeglądarkę internetową do:
         – zarządzania użytkownikami platformy i ich uprawnieniami (lekarze, pielęgniarki, ratownicy medyczni, Pacjenci i ich opiekunowie),

- administrowania urządzeniami,
- dodawanie / edytowanie danych Pacjenta,
- dodawania /edytowania urządzeń do telerehabilitacji.

c) Aplikacji mobilnej dla Pacjentów i ich opiekunów.

5) Usługowej platformy zaprojektowanej zgodnie z podejściem Data-First składającej się z silnika procesów pozwalającego na tworzenie przepływów sygnałów między Front Office, Back Office i oprogramowaniem warstwy przetwarzania danych oraz Urządzeń do telerehabilitacji.
6) API Gateway odpowiedzialnego za udostępnianie i zarządzanie usługami.
7) Warstwy dostępowej, odpowiadającej za fizyczne połączenie z Urządzeniami pracującymi zdalnie zgodnie z Architekturą Referencyjną. Oparta jest o sterowniki urządzeń. Wykonawca dostarcza sterownik dla dwóch rodzajów urządzeń do telerehabilitacji: EKG i opaska telemedyczna.
8) Warstwy przetwarzania danych składającej się z modułów:
   a) akwizycji danych – pobiera dane ze sterowników urządzeń i transformuje je do standardu zapisu, określonego w Architekturze Referencyjnej. Dane zbierane przez Moduł to na przykład:
      - EKG,
      - puls,
      - saturacja,
      - kroki,
      - lokalizacja urządzenia.
   b) wstępnego przetwarzania – usuwa ewentualny szum w danych, dba o przypisanie danych do Pacjenta,
   c) moduł monitoringu kardio – moduł do zarządzania urządzeniami do telerehabilitacji kardiologicznej, możliwość personalizacji zakresów alarmowych,
   d) moduł do analizy kardio – analiza wyników pomiarów EKG Pacjenta w ramach telerehabilitacji, analiza zdarzeń, tworzenie opisów i raportów,
   e) modułu wykrywania upadków – moduł wykrywający upadki z dokładnością 80%, oparty o algorytmy sztucznej inteligencji, uczące się podczas wykorzystywania Modułu. Oznacza to, że podczas testowania Systemu, 80% wykrytych upadków powinno być klasyfikowane przez osoby obsługujące System, jako prawidłowe wykrycie,
   f) modułu przewidywania sytuacji alarmowych – moduł oparty o algorytmy sztucznej inteligencji, uczące się podczas eksploatacji Modułu. Pracuje w tle i analizuje zebrane pomiary parametrów życiowych Pacjenta oraz wezwania pomocy, zapisane jako zasadne. Moduł ma za zadanie przewidywać zasadne wezwania na dwóch poziomach dokładności:
      - w przypadku, gdy Pacjent nawiązuje połączenie z Centrum Monitoringu, moduł ma za zadanie sklasyfikować nadchodzące do ratownika połączenie, jako zasadne lub niezasadne,
      - w przypadku, gdy moduł na podstawie parametrów życiowych wykryje zagrożenie zdrowia lub życia, ma za zadanie samoczynnie wywołać sygnał alarmowy na konsoli ratownika / lekarza, który nawiąże połączenie z pacjentem celem walidacji zagrożenia.
   g) analiza wyników – przegląd w formie graficznej (wykresy) i tabelarycznej wyników danego Pacjenta w zadanym przedziale czasu,
   h) plan telerehabilitacji – zestaw ćwiczeń w formie wideo do wykonania przez Pacjenta w domu przed komputerem lub tabletem, w którym odpowiednie algorytmy zaszyte w Systemie, za pośrednictwem urządzeń do telerehabilitacji, będą analizować ćwiczącego Pacjenta. Pacjent będzie zaznaczał, że wykonał poszczególne ćwiczenia, zlecone przez personel medyczny. Po wykonaniu zestawu ćwiczeń personel medyczny będzie miał możliwość przeanalizowania wyników pomiarów zarejestrowanych przez urządzenia do telerehabilitacji. Moduł umożliwia opis badań EKG oraz ich archiwizację,
   i) moduł edukacyjny – będzie zbiorem materiałów edukacyjnych, webinariów przeznaczonych dla Pacjentów oraz ich rodzin i bliskich.

5. Wymagania techniczno – funkcjonalne Modułu Telerehabilitacji

Lp.	Parametr wymagany
WT_1	Każdy Pacjent musi posiadać własny profil w Systemie- Kartę użytkownika, w którym Zamawiający może umieścić podstawowe informacje o Pacjencie, przypisanym urządzeniu do telerehabilitacji oraz indywidualnym planie telerehabilitacji.
WT_2	Funkcjonalność budowania bazy danych o Pacjentach „Karta pacjenta”: 1. Podstawowa baza danych takich jak: imię, Nazwisko, adres, PESEL, wiek, telefony kontaktowe do Użytkownika i opiekunów itp. (możliwość dokładania kolejnych pól danych, o dowolnej nazwie przez administratora). 2. Baza danych medycznych o stanie zdrowia zebranych podczas wywiadu o chorobach, zażywanych lekach, uczuleniach, itp. (możliwość dokładania kolejnych pól danych o dowolnej nazwie przez administratora). 3. Rejestr pomiarów wykonanych przez urządzenia do telerehabilitacji. 4. Rejestr Zdarzeń. 5. Plan do telerehabilitacji do wykonania w warunkach domowych z komputerem lub tabletem. 6. Moduł edukacyjny. Dodatkowo możliwość podpinania skanowanych dokumentów.
WT_3	Wyszukiwanie Pacjentów po: identyfikatorze urządzenia do telerehabilitacji, imieniu, nazwisku, organizacji, numerze telefonu.
WT_4	Dodawanie organizacji i przypisywania dla danych Pacjentów z możliwością późniejszego przefiltrowania np. organizacji i wszystkich przypisanych do niej Użytkowników urządzeń do telerehabilitacji oraz możliwość dodania konta w Systemie i przypisania mu uprawnień tylko dla danej swojej organizacji.
WT_5	Konfigurowanie każdego zintegrowanego z Systemem urządzenia do telerehabilitacji za pośrednictwem Systemu wg indywidualnych potrzeb danego Pacjenta.
WT_6	System zapewnia opiekunom Pacjentów, konsultantom Centrum Monitoringu oraz administratorom wywoływanie lokalizacji urządzenia do telerehabilitacji. System wyświetla pozycję Użytkownika w postaci ikony na mapach, wyświetlając koordynaty geograficzne oraz na żądanie adres administracyjny.
WT_7	System musi być zaprojektowany w sposób zapewniający gromadzenie danych w tym danych medycznych (wrażliwych) w sposób bezpieczny zgodny z ogólnymi przepisami i rozporządzeniami w zakresie Cyberbezpieczeństwa i rekomendacjami dotyczącymi przetwarzania dokumentacji medycznej w postaci elektronicznej.
WT_8	System musi zapewniać możliwość integracji z RREDM oraz migracji danych do innych systemów w razie potrzeby poprzez przejrzystą i udokumentowaną strukturę bazy danych, moduł exportu danych zgromadzonych w systemie w szczególności danych Użytkowników do formatu XML lub innego. Dodatkowo dane skanowane muszą być gromadzone w plikach graficznych o powszechnych formatach, a w ich nazwie muszą być zaszyte identyfikatory Pacjentów, których dotyczą te pliki.
WT_9	System musi umożliwiać określenie uprawnień na bazie ról minimum w zakresie: 1. Administrator – pełen dostęp, pełna konfiguracja systemu i swobodnego nadawania uprawnień dla pozostałych ról, 2. Koordynator – pełny dostęp do bazy danych jw. + możliwość generowania raportów i zestawień, dostęp do nagrań z wykonanych z/do Centrum Monitoringu. 3. Operatorzy: 1) Lekarz – Ratownik (konsultant)- dostęp do danych Pacjentów, Organizacji i przypisanych do nich Pacjentów, możliwość podglądu Karty pacjenta, edycji poszczególnych danych w Karcie pacjenta, do których zostały nadane uprawnienia przez Administratora Systemu, możliwość podglądu i opisywania wyników pomiarów wykonanych u Pacjentów przez urządzenia do telerehabilitacji, obsługa alarmów ze zintegrowanych urządzeń do telerehabilitacji, 2) Pielęgniarka – dostęp do danych Pacjentów, możliwość podglądu Karty pacjenta, edycji poszczególnych danych w Karcie pacjenta, do których zostały nadane uprawnienia przez Administratora Systemu, możliwość podglądu wyników pomiarów i ich opisów wykonanych u Pacjentów przez urządzenia do telerehabilitacji z możliwością generowania ich wydruków, obsługa alarmów ze zintegrowanych urządzeń do telerehabilitacji,

	3) Ratownik (konsultant) – dostęp do danych Pacjentów, możliwość podglądu Karty pacjenta, edycja poszczególnych danych w Karcie pacjenta, do których zostały nadane uprawnienia przez Administratora Systemu, obsługa alarmów ze zintegrowanych urządzeń do telerehabilitacji, opisywanie Zdarzeń, 4) Operator techniczny – dostęp do danych Pacjentów w Systemie, możliwość dodawania nowych Pacjentów, edycji danych, możliwość podglądu i opisywania wyników pomiarów wykonanych przez urządzenia do telerehabilitacji w Systemie, obsługi alarmów wygenerowanych ze zintegrowanych urządzeń do telerehabilitacji, 5) Organizacja – dostęp do Kart pacjentów danej instytucji, 6) Pacjent – dostęp do swoich danych zapisanych w Karcie Pacjenta – tylko do podglądu, dostęp do planu telerehabilitacji, Pacjent będzie zaznaczał, że wykonał poszczególne, zlecone przez lekarza ćwiczenia. Po wykonaniu zestawu ćwiczeń lekarz przeanalizuje wyniki badań zarejestrowane przez urządzenia do telerehabilitacji, a ich opis, wykonany przez lekarza będzie widoczny w Karcie pacjenta, dostęp do modułu edukacyjnego, 7) Opiekun – dostęp do danych swojego podopiecznego zapisanych w Karcie Pacjenta (bez danych wrażliwych) – tylko do podglądu, dostęp do planu telerehabilitacji, dostęp do modułu edukacyjnego.
WT_10	Funkcjonalności niezbędne do zapewnienia integracji z zestawami do telerehabilitacji i zapewnienie integralności danych: 1. Indywidualny numer Użytkownika urządzenia do telerehabilitacji, którym oznaczane będą wszelkie rekordy w bazie oraz dołączana dokumentacja skanowana. 2. Powiązanie Karty Pacjenta z unikalnym identyfikatorem urządzenia do telerehabilitacji w celu umożliwienia automatycznego otwarcia Karty użytkownika u operatora Centrum Monitoringu, do którego trafiło to połączenie (funkcja integracji z centralką IP PBX), po wykryciu Zdarzenia. 3. Powiązanie z innymi numerami (telefon stacjonarny, komórkowy), z których Użytkownik może dzwonić do Centrum Monitoringu z pozostałymi sprawami, w celu umożliwiania automatycznego otwarcia Karty użytkownika u operatora Centrum Monitoringu, do którego trafiło połączenie od Pacjenta (funkcja integracji z centralką IP PBX).
WT_11	Opisywanie przez lekarza wyników pomiarów EKG wykonanych samodzielnie przez Pacjenta w module analizy kardio. Wyniki po ich wykonaniu przesyłane są do modułu monitoringu kardio.
WT_12	Opisywanie Zdarzeń z odebranych połączeń od Pacjentów do Centrum Monitoringu przez ratowników i pracowników technicznych. Zdarzenie jest automatycznie rejestrowane i dopisywane do rejestru zdarzeń w Karcie pacjenta z możliwością oznaczenia: zasadne, techniczne, fałszywe, porada i sporządzenia notatki przez Operatora (np. stwierdziłem zagrożenie życia – wezwałem karetkę albo np. potrzebna pomoc). Po połączeniu do kolejnego Operatora, tworzy się historia obsługi tego zdarzenia w systemie przez kolejnych Operatorów z możliwością zapisania notatki przez każdego z nich (np.: udzieliłem porady, zaleciłem itp.).
WT_13	Podgląd zaimplementowanych do Systemu urządzeń do telerehabilitacji z poziomu konta administratora, koordynatora, lekarza, pielęgniarki, ratownika medycznego, pracownika technicznego. Po zalogowaniu się do Systemu na ekranie wyświetla się w formie listy statusów urządzeń do telerehabilitacji tj. imię i nazwisko Pacjenta, lokalizacja, numer telefonu. W zależności od sytuacji przewiduje się następujące rodzaje statusów urządzeń do telerehabilitacji rozróżnianych kolorami – zielony – urządzenie działa prawidłowo, szary – urządzenie nieaktywne z możliwością pozostawienia komentarza powodu nieaktywności powyżej określonego w systemie czasu np. po dobie, kolor czerwony – nagłe wyłączenie urządzenia do telerehabilitacji z Modułu poprzez np. wyczerpanie baterii lub brak komunikacji. Określenie czasu występowania danych statusów będzie mógł konfigurować Administrator Systemu.
WT_14	Monitorowanie z poziomu Systemu stanu naładowania baterii urządzeń do telerehabilitacjii, podglądu lokalizacji GPS, siły sygnału GSM i innych parametrów wysyłanych przez urządzenia do telerehabilitacji do Systemu, w tym informowanie alarmem technicznym, gdy stan baterii urządzenia spada poniżej 15% (parametr konfigurowalny przez Administratora).
WT_15	Prezentowanie historii wykonanych pomiarów przez urządzenia do telerehabilitacji danego Pacjenta. Lekarz ma dostęp do wszelkich pomiarów wykonanych samodzielnie przez Pacjenta wraz z ich opisem.
WT_16	Prezentowanie historii zdarzeń dotyczących danego Pacjenta (niezależnie czy dzwonił z urządzenia do telerehabilitacji, telefonu Pacjenta). Operator widzi listę pełnej historii zdarzeń z datą i godziną.
WT_17	Przyjmowanie połączeń przychodzących o Zdarzeniach na numer alarmowy Centrum Monitoringu.

WT_18	Wizualna informacja na ekranie wraz z sygnałem dźwiękowym i natychmiastowym otwarciem karty Pacjenta, który wywołał połączenie alarmowe, u operatora Centrum Monitoringu, który przyjął alarm.
WT_19	Tryb odpytywania Urządzenia do telerehabilitacji w momencie Zdarzenia i raportowanie lokalizacji Urządzenia na bieżąco.
WT_20	Akustyczne potwierdzenie połączenia odebranego przez System o Zdarzeniu z Urządzenia na stanowisku operatora.
WT_21	System ma umożliwić administratorowi ustawienie trybu monitorowania alarmów dla dowolnie wybranego użytkownika posiadającego odpowiednie uprawnienia w trybie: 1. śledzenia alarmów o zagrożeniu życia i zdrowia Pacjentów oraz alarmów technicznych, dotyczących stanu technicznego urządzeń do telerehabilitacji, 2. nadejście alarmu sygnalizowane jest w Centrum Monitoringu wyświetleniem w widoku alarmów systemu oraz sygnałem dźwiękowym połączenia przychodzącego. Po przyjęciu zgłoszenia przez pracownika Centrum Monitoringu następuje bezpośrednie połączenie głosowe z zintegrowanego przez API urządzenia do telerehabilitacji z operatorem Centrum Monitoringu, 3. alarmy o Zdarzeniach są sygnalizowane sygnałem dźwiękowym, który można dezaktywować, 4. informacja o alarmie musi zawierać: – pełną identyfikację urządzenia, z którego alarm został wygenerowany, wyświetlając dokładny czas alarmu, informacje o urządzeniu, z którego został wywołany alarm: poziom naładowania baterii, ostatnią dostępna lokalizację urządzenia na mapie wraz z opcją jej aktualizacji i wyświetlania za pomocą przycisku, pozostałe wyniki pomiarów, które umożliwia urządzenie (np. puls, ciśnienie, temperatura, saturacja, ilość wykonanych kroków), 5. jednoznaczną identyfikację użytkownika urządzenia, który wygenerował alarm, wraz z dostępem do karty informacyjnej o pacjencie.
WT_22	System zapewni definiowanie stref bezpieczeństwa, w których Pacjent może się poruszać. Zasięg stref jest wyświetlany na mapach Google. Wyjście Pacjenta z założonym urządzeniem do telerehabilitacji poza strefę jest sygnalizowane alarmem oraz wysyłane jest powiadomienie do opiekunów zgodnie z wcześniej zaprogramowanym algorytmem.
WT_23	System dostarczony w modelu usługowym SaaS (oprogramowanie jako usługa w chmurze).
WT_24	Funkcjonalność wyświetlania listy wszystkich operatorów, aktualnie zalogowanych w Systemie, wraz z numerem stanowiska i możliwością przełączenia do nich rozmowy z Pacjentem. Lista powinna pokazywać aktualny status operatora: wolny, rozmowa, przerwa (status przerwa wciskane ręcznie, status wolny, rozmowa pobrany z centrali IP PBX).
WT_25	Funkcjonalność integracji z centralą IP PBX w zakresie dostępu do nagrań powiązanych ze zdarzeniami zarejestrowanymi w systemie (lub konkretnym Użytkownikiem) i ich wyszukiwaniu i odtwarzaniu z poziomu Modułu.
WT_26	Generator raportów według kryteriów (wiek, płeć, miejsce zamieszkania Użytkownika, urządzenia do telerehabilitacji, gmina, powiat, typy Zdarzeń – alarmowe, techniczne, inne, urządzenie aktywne / nieaktywne z datą od kiedy brak kontaktu z Systemem, z możliwością modyfikowania kryteriów raportów, filtrowania i sortowania, zestawienia wykonanych pomiarów z urządzeń do telerehabilitacji dla danego Pacjenta w określonym przedziale czasowym.
WT_27	Zapewnienie możliwości rejestracji rozmów przychodzących i wychodzących z możliwością dostępu do odsłuchania nagrania z poziomu Systemu niezależnie od zalogowanego konta użytkownika.
WT_28	Zapewnienie integracji systemu z centralą VOIP i telefonami IP
Lp.	**Parametry dodatkowe**
WT_29	System posiada interfejs integracji poprzez API z urządzeniami zewnętrznymi do świadczenia usług telerehabilitacji np. funkcjonalność odczytu parametrów, EKG, opaski telemedycznej.
WT_30	Wykonawca dostarczy pięć aparatów do rejestracji i transmisji bezprzewodowej zapisu EKG, będący wyrobem medycznym, zintegrowanych z Modułem. Rejestrator zapewni: – rejestrowanie zdarzeń i zdalne monitorowanie pracy serca, – wykonywanie EKG metodą holtera, – wodoodporność na poziomie min. 67, – jednorazowe diody zatrzaskowe. Wykonawca udziela nieodpłatnej gwarancji na urządzenie przez okres 24 miesięcy.
WT_31	Wykonawca dostarczy pięć opasek telemedycznych, zintegrowanych z Modułem. Opaska posiada następujące parametry:

	– wbudowany wyświetlacz, – ładowarka magnetyczna, – wodoszczelność na poziomie min. IP 66, – pomiar tętna i saturacji, – możliwość wykonywania i odbierania połączeń telefonicznych, umożliwiający dwukierunkową komunikację głosową, – wyróżniony przycisk dedykowany do wywołania sygnału alarmowego, – urządzenie posiada certyfikat CE. Wykonawca udziela nieodpłatnej gwarancji na urządzenie przez okres 24 miesięcy.

6. Dokumentacja

Lp.	Parametr wymagany
WT_32	Na początku realizacji niniejszego Zamówienia Wykonawca przedstawi propozycję zakresu dokumentacji oraz kryteria ich odbioru. Propozycja ta, po zaakceptowaniu przez Zamawiającego będzie podstawą do odbioru poszczególnych elementów dokumentacji.
WT_33	Na początku realizacji niniejszego Zamówienia Wykonawca przedstawi propozycję Planu Wdrożenia. Propozycja ta, po zaakceptowaniu przez Zamawiającego będzie podstawą do odbioru poszczególnych etapów Zamówienia.
WT_34	Wykonawca będzie zobowiązany do dostarczenia propozycji dokumentacji wskazanej powyżej, w pkt. WT_32 i WT_33, w terminie do 14 dni roboczych od daty zawarcia Umowy. Zamawiający dokona weryfikacji otrzymanej propozycji w terminie do 3 dni od daty jej otrzymania od Wykonawcy. W przypadku braku zgłoszenia uwag przez Zamawiającego w tym terminie Wykonawca będzie mógł uznać, że Zamawiający zaakceptował propozycje dokumentacji wskazanej w pkt. WT_32 i WT_33 i będzie to dokument obowiązujący w trakcie realizacji przedmiotu zamówienia. W przypadku uwag Zamawiający przedstawi je Wykonawcy i wyznaczy dodatkowy min. 10 dniowy termin na uwzględnienie ich w propozycji dokumentacji. Zamawiający dokona weryfikacji zgodnie z procedurą określoną w zdaniu drugim.
WT_35	Plan Wdrożenia będzie stanowił dokument określający sposób realizacji przedmiotu Umowy, w tym kryteria odbioru produktów wdrożenia i będzie stanowił podstawę do przeprowadzenia przez Zamawiającego kontroli realizacji przedmiotu Umowy. Składowymi Planu Wdrożenia powinny być między innymi: 1) Struktura zespołu realizującego zamówienie, 2) Harmonogram realizacji prac. Testy i terminy zgodne z wyznaczonymi ramami czasowymi projektu, dla wszystkich elementów harmonogramu (czas rozpoczęcia i czas zakończenia).
WT_36	W ramach Projektu Technicznego Wykonawca przedstawi ogólny i szczegółowy Opis architektury oraz całego rozwiązania i powiązania z systemami zewnętrznymi: 1) założenia i ograniczenia, 2) uwzględnienie aspektów wydajności i bezpieczeństwa, 3) charakterystyka użytkowników narzędzia telerehabilitacji, 4) ustalenie zakresu danych wprowadzanych do systemów, 5) szczegółowe wymagania dotyczące środowiska systemów, 6) identyfikację źródeł danych do celów zasilania systemów danymi, 7) formaty obsługiwanych danych, 8) opis parametrów, które mogą ulec zmianie w trakcie realizacji zadania lub są wymagane do poprawnej pracy wdrażanego systemu. Zastosowane rozwiązania muszą spełniać wszystkie wymagania Zamawiającego.
WT_37	1. Wykonawca opracuje i dostarczy Zamawiającemu dokument Plan Testów. 2. Dokument Plan Testów musi być dostosowany do Harmonogramu realizacji Zamówienia oraz musi uwzględniać testy dla wszystkich komponentów wdrożonych w ramach realizacji niniejszego Zamówienia. 3. Dokument Plan Testów musi zawierać: 1) opis sposobu organizacji testów z uwzględnieniem terminów, lokalizacji, wymaganego narzędzia analitycznego, 2) szablon listy uczestników z podziałem na role/funkcje podczas trwania testów, 3) rodzaje przeprowadzanych testów, 4) dane testowe (opis danych, źródło pochodzenia itp.), 5) opis sposobu rejestracji przebiegu i wyników testów,

	6) testy funkcjonalne, polegające na testowaniu produktów od strony użytkownika, tzw. metoda czarnej skrzynki. 4. Dokument Plan Testów musi uwzględniać testy: 1) akceptacyjne, 2) wydajnościowe. 5. Zadaniem testów akceptacyjnych jest dokonanie oceny kryteriów jakościowych i weryfikacja zaimplementowanych funkcjonalności z wyspecyfikowanymi wymaganiami oraz sprawdzenie kompletności nawigacji w systemach. 6. Zamawiający ma prawo do samodzielnej weryfikacji prawidłowości wykonania usługi poprzez zdefiniowanie własnych, dodatkowych scenariuszy testowych. 7. Wykonawca musi przeprowadzić testy akceptacyjne w siedzibie Zamawiającego. 8. Wykonawca musi rejestrować podczas testów wszystkie wykryte błędy, kategorie błędu oraz liczbę błędów wykrytych podczas testów. 9. Wykonawca musi opracować Raport z testów obejmujący co najmniej: 1) opis miejsca i termin przeprowadzenia testów, 2) listę osób biorących udział w testach, 3) opis środowiska testowego, 4) listę zrealizowanych scenariuszy testowych, 5) listę zrealizowanych przypadków testowych w ramach scenariuszy testowych, 6) wynik realizacji poszczególnych przypadków testowych i scenariuszy testowych, 7) listę zgłoszonych uwag wraz z adnotacją o sposobie i terminie usunięcia niezgodności. W raporcie z testów akceptacyjnych (testowanie wersji produkcyjnych systemów) wszystkie testy muszą zakończyć się wynikiem pozytywnym.
WT_38	W ramach realizacji Przedmiotu Zamówienia Wykonawca zobowiązany jest do opracowania Dokumentacji powykonawczej zawierającej m.in.: 1) opis architektury, 2) zaktualizowany projekt techniczny systemów, 3) opis wykonanych instalacji technicznych, 4) instrukcje techniczno-instalacyjne, 5) schemat struktury danych, 6) podręcznik użytkownika (User Guide) opisujący sposób użycia poszczególnych funkcji Systemu, 7) procedury działania administratora Systemu, 8) procedury związane z wykonaniem kopii zapasowych systemów, 9) procedury związane z odtworzeniem systemów z kopii zapasowych, 10) Dokumentacja z wykonanych testów, 11) wytyczne dot. narzędzi programistycznych, 12) Kody źródłowe.
WT_39	Wykonawca zobowiązany jest zapewnić w ramach realizacji Przedmiotu Zamówienia wszelkie prawa umożliwiające Zamawiającemu korzystanie z opracowanej oraz dostarczonej w ramach realizacji Dokumentacji.
WT_40	Dokumentacja związana z Zamówieniem musi być sporządzona w języku polskim i dostarczona w wersji elektronicznej w pliku w formacie pdf i wersji edytowalnej oraz w wersji papierowej oznaczonej numerem wersji, datą wersji oraz z dołączoną tabelą rejestracji zmian.
WT_41	Zamawiający wymaga, aby wszystkie dokumenty tworzone w ramach realizacji Umowy charakteryzowały się wysoką jakością, na którą będą miały wpływ takie czynniki jak: 1) Struktura dokumentu, rozumiana, jako podział danego dokumentu na rozdziały, podrozdziały i sekcje, w czytelny i zrozumiały sposób, 2) Zachowanie standardów, w tym notacji UMWK-P, a także sposób pisania, rozumiany, jako zachowanie spójnej struktury, formy i sposobu pisania dla poszczególnych dokumentów oraz fragmentów tego samego dokumentu, 3) Kompletność dokumentu, rozumiana, jako pełne, bez wyraźnych, ewidentnych braków przedstawienie omawianego problemu obejmującego całość z danego zakresu rozpatrywanego zagadnienia.

7. Przekazanie Kodów źródłowych

Celem jest przekazanie Zamawiającemu przez Wykonawcę Kodów źródłowych Produktów (programów komputerowych wchodzących w skład Systemu wytworzonego w wyniku realizacji Umowy oraz skryptów konfiguracyjnych).

Lp.	Parametr wymagany
WT_42	Wykonawca przekaże Zamawiającemu nośniki z Kodami źródłowymi Systemu zawierające archiwa w formacie *.zip: 1. wersje źródłowe Systemu wraz z niezbędnymi elementami, zawierające w szczególności: 1) programy napisane w językach programowania (np. Java), 2) skrypty (np. do kompilacji, migracji baz danych), 3) zastosowane biblioteki oprogramowania, 4) komplet definicji obiektów wytworzonych i uruchamianych z wykorzystaniem oprogramowania standardowego, 5) definicje modeli danych, 6) wszelkie definicje niezbędne dla współdziałania oprogramowania z otoczeniem, 2. dokumentację zawierającą co najmniej: 1) wykaz przekazywanych elementów wchodzących w skład Kodów źródłowych, 2) wykaz zmian i rozszerzeń w stosunku do poprzedniej wersji przekazanych Kodów źródłowych w postaci listy zmian funkcjonalności wraz z poprawkami, 3) instrukcję kompilacji Kodów źródłowych, 4) instrukcję instalacji wraz z zestawieniem użytych parametrów konfiguracyjnych umożliwiającą konfigurację środowiska.

8. Wymogi w zakresie architektury teleinformatycznej

1. Wykonawca jest zobowiązany dostarczyć środowisko teleinformatyczne HA w modelu chmury obliczeniowej, oferowane z infrastruktury CPD wraz z niezbędnym oprogramowaniem, w tym min.:
   1) skonfigurować i udostępnić infrastrukturę teleinformatyczną CPD wraz z niezbędną mocą obliczeniową i przestrzenią dyskową oraz oprogramowaniem zgodnie z określonymi przez Zamawiającego wymaganiami, w terminie do 5 dni roboczych od dnia podpisania Umowy,
   2) skonfigurować i utrzymywać połączenia sieciowe pomiędzy poszczególnymi instancjami serwerowymi,
   3) skonfigurować i udostępnić dedykowane łącza telekomunikacyjne zgodnie z określonymi w SWZ minimalnymi parametrami pozwalającymi w sposób niezakłócony realizować usługi ze wszystkich instancji serwerowych zlokalizowanych w środowisku teleinformatycznym dostarczonym przez Wykonawcę,
   4) skonfigurować i udostępnić łącza do sieci Internet, zgodnie z określonymi w SWZ minimalnymi parametrami pozwalającymi w sposób niezakłócony realizować usługi ze wszystkich instancji serwerowych zlokalizowanych w środowisku teleinformatycznym dostarczonym przez Wykonawcę,
   5) skonfigurować i utrzymywać ochronę na styku z Internetem w warstwie sieciowej i aplikacyjnej,
   6) skonfigurować i utrzymywać na każdej instancji serwerowej oprogramowanie antywirusowe aktualizowane na bieżąco, zarządzane z jednej konsoli administracyjnej, zabezpieczającej przed wirusami, robakami, malewarem, ransomwarem, rootkitami i innymi zagrożeniami należącymi do kategorii zagrożeń wirusowych systemów informatycznych,
   7) zapewnić niezbędne oprogramowanie związane z realizacją zamówienia,
   8) zapewnić system zbierania i przechowania logów zdarzeń z urządzeń sieciowych w celu stałego monitorowania wydajności rozwiązania,
   9) świadczyć pełną obsługę administrowania uruchomionymi instancjami serwerowymi,
   10) dostarczyć usługę backupu wszystkich maszyny wirtualnych będących składnikami dostarczonego środowiska teleinformatycznego,
   11) zapewnić pełne wsparcie eksperckie, merytoryczne i administracyjne w zakresie utrzymania systemu backupu, kreowania polityk kopii zapasowych zgodnie z wymogami Zamawiającego, utrzymywania

i zarządzania całością systemu backupu, zgodnie z najlepszymi praktykami, jak również wytycznymi z audytów przeprowadzanych przez instytucje zewnętrzne, którym podlega Zamawiający przez cały okres realizacji usługi;

2. Zamawiający wymaga, aby całość usługi była realizowana z infrastruktury jednego CPD, a serwery, na których będą umieszczone dane muszą podlegać prawu europejskiemu.
3. Wykonawca zobowiązany jest wskazać w ofercie lokalizację gromadzonych i przetwarzanych danych będących przedmiotem Umowy (nazwa i adres CPD) .
4. Zamawiający z uwagi na ograniczenie ryzyka związanego z wydłużonym czasem dojazdu do CPD na wypadek awarii lub innych zdarzeń, zastrzega, że odległość pomiędzy siedzibą Zamawiającego, a CPD nie może być większa niż 50 km (średni czas dojazdu do 1h).
5. Zamawiający oczekuje ustawienia realizacji harmonogramu retencji backupu:
   1) tygodniowa – 7 dni,
   2) miesięczna – 30 dni.
6. Zamawiający oczekuje realizacji wykonywania kopii zapasowych w godzinach od 22.00 do 6.00 dnia następnego.
7. Zamawiający oczekuje konsoli do samodzielnego zarządzania backupem z przeszkoleniem osoby/osób oddelegowanej/ych przez Zamawiającego do zarządzania backupem.
8. Zamawiający oczekuje monitoringu backupu, który charakteryzuje się następującymi parametrami:
   1) interwały sprawdzania poprawności działania usługi powinny być częstsze niż 5 min,
   2) system musi w czasie rzeczywistym informować o aktualnym stanie kopii zapasowej,
   3) system musi w czasie rzeczywistym raportować o wolnej przestrzeni dyskowej,
   4) system musi w czasie rzeczywistym monitorować wszystkie ustalone z Wykonawcą w trakcie wdrożenia parametry usługi, jak np. czas wykonania kopii zapasowej, czy ilość przetworzonych danych (rozmiar).
9. Zamawiający oczekuje dostarczenia rozwiązania, które w sposób automatyczny będzie testowało w sposób jednoznaczny poprawność wykonania kopii zapasowej.
10. Zamawiający oczekuje dostarczenia rozwiązania, które w sposób zautomatyzowany dokona testowego odtworzenia kopii zapasowej i weryfikacji spójności wszystkich odtwarzanych danych.
11. Zamawiający oczekuje możliwości realizacji testowego odtworzenia kopii zapasowej z częstotliwością nie częściej niż raz w miesiącu przez Wykonawcę na żądanie Zamawiającego, w środowisku chmury obliczeniowej dostarczonym przez Wykonawcę w ramach niniejszego zamówienia.
12. Zamawiający oczekuje realizacji RTO na poziomie 6 h dla całego środowiska oraz RPO zgodnie z przyjętym harmonogramem.
13. Wykonawca zobligowany jest do dostarczenia backupu, który posiada następujący minimalny zestaw funkcjonalności w ramach dostarczonego rozwiązania:
   1) rozwiązanie musi umożliwiać odtworzenie całej maszyny wirtualnej, jak również pojedynczych plików bezpośrednio z kopii zapasowej (bez konieczności przywracania w całości maszyny wirtualnej, aby odzyskać pojedynczy plik), niezależnie od systemu operacyjnego maszyny wirtualnej,
   2) rozwiązanie musi być wyposażona w wewnętrzne mechanizmy kompresji i deduplikacji- wykluczone jest stosowanie narzędzi innych, niż producenta rozwiązania systemu kopii zapasowej,
   3) mechanizm kompresji i deduplikacji musi być dostępny tylko dla danych nie zaszyfrowanych zarówno po stronie systemu operacyjnego maszyn wirtualnych i serwerów fizycznych oraz zaszyfrowanych przez dostarczony system kopii zapasowych,
   4) rozwiązanie musi umożliwiać pełne uruchomienie maszyny wirtualnej z kopii zapasowej w przypadku awarii oraz równoczesną realizację jej przywracania. Równolegle muszą mieć możliwość działać dwa procesy:
      a) proces przywracania maszyny wirtualnej z kopii zapasowej;
      b) proces jej poprawnego, pełnego funkcjonowania w trakcie operacji przywracania,
   5) rozwiązanie musi umożliwiać przywracanie pojedynczych elementów aplikacyjnych z kopii zapasowych bez konieczności wcześniejszego przywrócenia całej maszyny wirtualnej.

9. Wymogi w zakresie przetwarzania danych

1. Z uwagi na potrzebę wysokiej dostępności całej usługi będącej przedmiotem zamówienia wraz z wszystkimi systemami towarzyszącymi, Zamawiający oczekuje, aby proponowane rozwiązanie spełniało najwyższe, dostępne na terenie Unii Europejskiej standardy bezpieczeństwa informatycznego. Wymagania dla CPD są obligatoryjne. Wykluczone jest częściowe spełnianie któregokolwiek wymogu. Zamawiający na etapie wyboru oferty, a także realizacji usługi zastrzega możliwość weryfikacji i udokumentowania spełniania każdego z wymogów CPD.
2. Zamawiający oczekuje, że CPD posiada odpowiednie zabezpieczenia fizyczne i organizacyjne zapewniające bezpieczeństwo przetwarzanych danych Zamawiającego. Wykonawca ponosi odpowiedzialność w zakresie bezpieczeństwa informacji i danych przechowywanych na wykorzystanej infrastrukturze teleinformatycznej CPD.
3. Zamawiający oczekuję, że CPD posiada wysokie bezpieczeństwo sprzętu teleinformatycznego w postaci m.in.:
   1) izolacji sprzętu krytycznego (dedykowana przestrzeń wyłącznie dla urządzeń serwerowych),
   2) ochrony przed uszkodzeniem infrastruktury serwerowej w postaci zamykanych szaf rack,
   3) prowadzenia rejestru wejść i wyjść do obszaru, w którym umieszczony jest sprzęt przeznaczony do obsługi Zamawiającego.
4. Zamawiający oczekuje, że CPD zapewnia profesjonalne utrzymanie i konserwację wykorzystywanej infrastruktury, w postaci m.in:
   1) posiadania i stosowania procedury kontroli, regularnych przeglądów zgodnie z zaleceniami producentów, konserwacji i naprawy sprzętu teleinformatycznego, energetycznego i klimatyzacyjnego,
   2) napraw dokonywanych przez personel posiadający kwalifikacje zgodnie z zaleceniami producenta sprzętu i wewnętrznymi procedurami lub autoryzowane serwisy zewnętrzne,
   3) usuwaniem nośników danych ze sprzętu teleinformatycznego przed przekazaniem do naprawy lub serwisu,
   4) stosowania bezpiecznej utylizacji lub przekazywania sprzętu do ponownego użycia, w tym skuteczne usuwanie danych z nośników (wraz z systemami operacyjnymi i danymi licencyjnymi),
   5) ochrony Zamawiającego przed instalacją złośliwego oprogramowania w udostępnionych Zamawiającemu usługach,
   6) prowadzenia aktualnego rejestru: przeglądów, incydentów, awarii i usterek.
5. Zamawiający oczekuje, że CPD musi spełniać poniższe wymagania (wymagania obligatoryjne):

L.p.	Parametr lub kryterium	Wyeliminowanie zagrożenia
OBIEKT I LOKALIZACJA		
1	CPD zlokalizowane na terenie UE lub Lichtensteinu, Islandii, Norwegii. Wszystkie dane Zamawiającego będą gromadzone i przetwarzane na terenie UE lub Lichtensteinu, Islandii, Norwegii.	Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium UE. Brak spełnienie wymagań RODO / GDPR.
2	CPD posiada ogrodzony zamknięty teren wraz z ograniczoną strefą wejść.	Brak podstawowej kontroli fizycznego dostępu do infrastruktury IT oraz innych urządzeń (elementy zasilania, chłodzenia, wentylacji).
3	CPD jest usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub zalanie.	Zagrożenie nieprzerwanej pracy infrastruktury IT oraz innych urządzeń (elementy zasilania, chłodzenia, wentylacji) w wyniku działań działania sił natury.
4	CPD jest położony nie mniej niż 5 metrów powyżej poziomu wody stuletniej	Zagrożenie długotrwałego zalania. Wysoka intensywność oddziaływania sytuacji krytycznych.

5	CPD jest oddalony nie mniej niż 1 km od składowisk lub fabryk produkujących materiały toksyczne, radioaktywne, wybuchowe, żrące, również od stacji paliw lub składowisk paliw płynnych oraz baz wojskowych.	Zagrożenie powstania sytuacji zagrażających zdrowiu lub życiu osób fizycznie obsługujących urządzenia, długotrwałego skażenia terenu lub długotrwałych działań służb zapobiegających zdarzeniom krytycznym (np. odcięcie terenu przez straż pożarną, wojsko). Zagrożenie fizycznego uszkodzenia infrastruktury IT oraz innych urządzeń w skutek eksplozji zewnętrznej.
6	CPD jest oddalony nie mniej niż 1 km od miejsc narażonych na wandalizm lub zamieszki (stadiony i obiekty sportowe, centra handlowe, miejsca organizacji imprez masowych dla 10 tys. osób i więcej).	Zagrożenie długotrwałego zablokowania dróg dojazdowych do ośrodka, ryzyko niekontrolowanego zachowania tłumów, ryzyko zamieszek, zniszczeń.
7	CPD nie posiada ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi, położonych nad pomieszczeniami z urządzeniami serwerowymi.	Zagrożenie przecieków, zalania infrastruktury IT lub nagłych zmian warunków środowiskowych pracy urządzeń (wzrost wilgotności).
8	CPD posiada nie mniej niż 15 metrów oddalenia urządzeń serwerowych udostępnionych Zamawiającemu od źródeł pól zakłócających takich jak transformatory SN i WN.	Zagrożenie uszkodzenia urządzeń i danych w wyniku niekorzystnego oddziaływania półzakłócających pracę urządzeń elektrycznych i magnetycznych.
9	CPD posiada pomieszczenia serwerowe o wysokości nie mniejszej niż 3,5 metra- wysokość mierzona od podłogi technicznej do sufitu pomieszczenia- w których będą znajdowały się urządzenia serwerowe udostępnione Zamawiającemu.	Zagrożenie zachowania odpowiedniej cyrkulacji powietrza, zachowania stref gorącej i zimnej, zmian parametrów środowiskowych. Zagrożenie uszkodzenia lub utraty danych na wypadek uruchomienia systemu gaszenia.
10	CPD posiada podłogę techniczną w pomieszczeniu z serwerami o wysokości nie mniejszej niż 1 metr.	Zagrożenie dla zachowania cyrkulacji powietrza w wyniku zablokowania przez instalacje podpodłogowe, brak miejsca dla instalacji podpodłogowych.
11	CPD spełnienia wymagania obowiązujących przepisów oraz europejskich i polskich norm w zakresie: budownictwa, energetyki oraz instalacji elektrycznych, BHP, ochrony przeciwpożarowej.	Przeciwdziałanie zagrożeniom budowlanym, pożarowym lub zagrożeniu życia i zdrowia ludzi w wyniku niezastosowania przepisów BHP, stosowania odrębnych od powszechnie stosowanych oznaczeń, błędów instalacji energetycznej.
WĘZŁY TELEKOMUNIKACYJNE		
1	CPD posiada połączenie światłowodowe z niezależnymi operatorami telekomunikacyjnymi, w tym nie mniej niż 2 operatorów o zasięgu krajowym jest podłączonych niezależnymi drogami światłowodowymi.	Zagrożenie awarii lub innej przyczyny zaprzestania świadczenia usług transmisji danych przez operatora zewnętrznego.
2	Dojścia połączeń CPD wykonane są dwoma niezależnymi trasami kablowymi.	Zagrożenie utraty ciągłości komunikacji danych z ośrodkiem.
3	CPD posiada węzeł dostępowy do sieci Internet dopięty do minimum 2 różnych operatorów z zaimplementowanym protokołem BGP.	Zapewnienie niezawodności i jakości transmisji danych w ramach sieci Internet. Przeciwdziałanie zagrożeniu utraty komunikacji z siecią Internet.
4	CPD posiada węzeł dostępowy do sieci Internet ze zdublowanymi urządzeniami o gwarancji dostępności rocznej usługi 99,99%.	Zagrożenie utraty ciągłości komunikacji sprzętu z siecią Internet.
5	CPD posiada węzeł telekomunikacyjny wyposażony w redundantny system firewall.	Zagrożenie utraty zabezpieczenia systemów informatycznych w wyniku uszkodzenia zapory ogniowej.

6	CPD posiada węzeł telekomunikacyjny wyposażony w redundantny system detekcji i prewencji włamań z sieci.	Zagrożenie bezpieczeństwa danych w wyniku ataku informatycznego na systemy.
ZASILANIE ENERGETYCZNE		
1	CPD posiada dostępność roczną systemu zasilania energetycznego na poziomie nie niższym niż SLA 99,999% w skali roku.	Zagrożenie ciągłości pracy urządzeń i dostępności urządzeń.
2	CPD posiada nie mniej niż dwie niezależne linie zasilania dostępne dla infrastruktury IT.	Zagrożenie zachowania ciągłości zasilania w wyniku uszkodzenia linii zasilającej lub długotrwałego przywracania ciągłości zasilania.
3	CPD posiada system zasilania awaryjnego UPS osobno na każdą linię zasilającą.	Zagrożenie dla zachowania nieprzerwanego zasilania urządzeń lub skrócenia pracy urządzeń na zasilaniu awaryjnym poniżej czasu bezpiecznego.
4	CPD posiada redundantny system agregatów prądotwórczych.	Zagrożenie braku zachowania zasilania.
5	System zasilaczy awaryjnych UPS w CPD gwarantuje podtrzymanie zasilania urządzeń serwerowych oraz infrastruktury towarzyszącej, przeznaczonej dla Zamawiającego przez przynajmniej 15 minut od zaniku napięcia i nie krócej niż do czasu uruchomienia się agregatów i ich synchronizacji z siecią energetyczną.	Zagrożenie ciągłości pracy urządzeń w wyniku niedostosowania czasu pracy na zasilaniu awaryjnym do czasu reakcji na awarię zasilania i uruchomienia agregatów. Zagrożenie dla utraty lub uszkodzenia danych w wyniku niedostosowania czasu pracy urządzeń do czasu bezpiecznego zamknięcia wykonywanych na urządzeniach procesów.
6	Agregaty prądotwórcze CPD posiadają zapas paliwa pozwalający na autonomiczną pracę bez konieczności uzupełniania zbiorników przez co najmniej 8 godzin. Agregat musi umożliwiać uzupełnienie paliwa w trakcie jego pracy.	Zagrożenie powstania przerw w zasilaniu wynikających z zatrzymania pracy agregatów.
BEZPIECZEŃSTWO		
1	CPD jest wyposażone w system sygnalizacji włamania i napadu, system wykrywania wody i zalania.	Zagrożenie braku kontroli i reakcji na naruszenie bezpieczeństwa fizycznego lub zalanie obiektu.
2	CPD posiada ochronę całego obiektu realizowaną przez profesjonalną zewnętrzną licencjonowaną firmę ochrony mienia. Ochrona realizowana jest w trybie 24/7.	Element zabezpieczenia bezpieczeństwa fizycznego ośrodka i zmniejszenia czasu interwencji wyspecjalizowanych służb w sytuacji kryzysowej.
3	CPD posiada system CCTV, który zapewnia ciągły 24/7 dozór obszarów i rejestrację zdarzeń z zachowaniem następujących parametrów funkcjonalnych: monitorowane wszystkie wejścia do obiektu – kamery wewnętrzne, monitorowane wszystkie pomieszczenia technologiczne.	Element zapewnienia wczesnego wykrywania i ostrzegania przed zagrożeniem naruszenia bezpieczeństwa fizycznego obiektu oraz zabezpieczenia materiału dowodowego na wypadek zaistnienia naruszenia, w tym identyfikacji osób.
4	System CCTV w CPD powinien zapewnić: rejestrację z zapisem aktualnej daty i godziny, archiwizacja zapisanego materiału przez okres nie krótszy niż 14 dni.	Element zapewniający możliwość określenia chronologii zdarzeń zapisanych w systemie monitorującym oraz odtworzenie zapisu zdarzeń po wykryciu zagrożeń.
5	System SKD (System Kontroli Dostępu) w CPD obejmuje nie mniej niż cztery strefy dostępu.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. Element wymuszający weryfikację kontroli poziomów uprawnień osób poruszających się po terenie i obiekcie.

6	Dostęp do strefy I (teren w otoczeniu obiektu) w CPD podlega identyfikacji na podstawie dokumentu tożsamości (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów) wkraczających na ogrodzony teren w otoczeniu obiektu.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.
7	Dostęp do strefy II (część biurowa obiektu) w CPD podlega identyfikacji na podstawie dokumentu tożsamości ze zdjęciem.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.
8	Dostęp do strefy III (strefa technologiczna) w CPD możliwy jest wyłącznie przy użyciu unikalnej i osobistej karty identyfikacyjnej współpracującej z SKD.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.
9	Dostęp do strefy IV (pomieszczenia ze sprzętem serwerowym Zamawiającego) w CPD możliwy jest wyłącznie przy użyciu łącznie 2 elementów identyfikacji: SKD, osobistej karty identyfikacyjnej, hasła (kodu) lub elementu biometrycznego.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.
10	CPD posiada system gaszenia bezpieczny dla ludzi i sprzętu komputerowego oraz serwerowego.	Zagrożenie powstania uszczerbku na zdrowiu lub życiu osób w wyniku funkcjonowania systemu gaszenia.
11	CPD posiada ściany, stropy części technologicznej o odporności ogniowej minimum 60 minut. Wszystkie drzwi prowadzące do pomieszczeń technologicznych o odporności ogniowej 60 minutowej.	Zapewnienie oporności ogniowej do czasu reakcji służb ratowniczych w celu ograniczenia skutków wystąpienia pożaru. Przeciwdziałanie zagrożenia rozprzestrzeniania się pożaru.
MONITORING		
1	CPD posiada elektroniczny system przyjmowania zgłoszeń dotyczących awarii dostępny w trybie 24/7.	Eliminacja zagrożenia braku działań reakcji na zdarzenia krytyczne przypadające poza godzinami pracy biurowej.
2	CPD posiada stałe i całodobowe 24/7 monitorowanie poprawności pracy infrastruktury i urządzeń komputerowych udostępnianej Zamawiającemu. Pomiary mają dotyczyć minimum: wykresy przebiegów temperatury, wykres przebiegu wilgotności.	Zagrożenie braku kontroli parametrów pracy ośrodka oraz długich reakcji niekorzystne zmiany warunków pracy urządzeń.

10. Wymogi w zakresie SLA

1. Z uwagi na potrzebę wysokiej dostępności usług będących przedmiotem zamówienia wraz z wszystkimi systemami towarzyszącymi, Zamawiający oczekuje, aby rozwiązanie spełniało wysoki poziom SLA, tj. nie mniej niż 99% w okresie realizacji Umowy oraz nieodpłatnej gwarancji. Wykonawca jest zobowiązany do przedstawienia raportu SLA w terminie 5 dni kalendarzowych od zakończenia okresu gwarancji.
2. Obsługa utrzymania i zarządzania oferowanego rozwiązania musi być realizowana w trybie 24/7/365.
3. Przyjmowanie zgłoszeń serwisowych musi być realizowane w trybie 24/7/365 w systemie online Wykonawcy, który umożliwia podgląd wszystkich dokonanych zgłoszeń, czas ich realizacji oraz bieżący ich status.

11. Wymogi w zakresie wsparcia i utrzymania

1. Do zadań realizowanych przez Wykonawcę w ramach usług utrzymaniowych infrastruktury informatycznej i wsparcia IT należy bieżąca obsługa administracyjna zasobów informatycznych (instancji serwerowych) zakresie:
   1) instalacji i konfiguracji systemów operacyjnych,

2) instalacji i konfiguracji elementów niezbędnych do zapewnienia środowiska wysokiej dostępności (HA),
3) aktualizacji oprogramowania ze względu na błędy bezpieczeństwa,
4) utrzymania infrastruktury pod kątem wydajności, bezpieczeństwa,
5) realizacji bieżących czynności administracyjnych,
6) analiz incydentów oraz problemów wraz z pełnym przywracaniem funkcjonalności.

12. Wymogi w zakresie połączeń sieciowych

1. Zamawiający ma obowiązek dostarczyć na potrzeby środowisk chmurowych łącza telekomunikacyjne pozwalające na płynne i bezpieczne działanie rozwiązania.
2. Wykonawca zapewni połączenie do sieci Internet dla dostarczanego rozwiązania za pomocą co najmniej 2 niezależnych operatorów telekomunikacyjnych o zasięgu co najmniej krajowym. Dostępna dla całej dostarczonej infrastruktury przepustowość łącza do Internetu musi wynosić co najmniej 1 Gbit/s (łącze symetryczne). Wykonawca do dostarczonych łączy do Internetu zapewni ochronę AntiDDoS w pełnym zakresie przepustowości dostarczanego w danym momencie łącza.

13. Zobowiązania Wykonawcy

1. Wykonawca udzieli Zamawiającemu pełnej informacji na temat stanu realizacji przedmiotu zamówienia, na każde wezwanie Zamawiającego.
2. Wykonawca zobowiązany będzie współdziałać z osobami wskazanymi przez Zamawiającego.
3. Zamawiający wymaga zatrudnienia przez Wykonawcę na podstawie umowy o pracę osób wykonujących w zakresie realizacji zamówienia czynności polegające na wykonywaniu pracy w sposób określony w art. 22 § 1 Ustawy z dnia 26 czerwca 1974 r.- Kodeks pracy (tj. Dz.U. z 2018r. poz. 917 z późn. zm.).
4. Wykonawca musi wdrożyć systemy w dwóch środowiskach:
   1) Produkcyjnym- środowisko, w którym będzie funkcjonowało rozwiązanie produkcyjnie. W środowisku tym będą tylko komponenty wykorzystywane produkcyjnie.
   2) Testowym- środowisko takie samo funkcjonalnie, jak środowisko produkcyjne, ale bez redundancji komponentów, odseparowane od niego – dedykowane do testów funkcjonalnych oraz testowania poprawek, zmian i rozszerzeń. Środowisko testowe dostępne będzie dla Zamawiającego od dnia wystawienia przez Wykonawcę pierwszej wersji Systemu.
5. Wykonawca musi opracować i wdrożyć procedury zachowania spójności pomiędzy środowiskami (produkcyjnym i testowym) w zakresie konfiguracji systemu oraz danych. Konfiguracja środowiska testowego powinna odzwierciedlać środowisko produkcyjne w zakresie umożliwiającym wykonanie procedur testowych.
6. Systemy muszą być zbudowane z wykorzystaniem technologii i narzędzi zapewniających stabilność, wydajność, skalowalność oraz bezpieczeństwo. Zamawiający wymaga, aby wykorzystane technologie były sprawdzone i nowoczesne, udokumentowane oraz powszechnie wykorzystywane.
7. Wykonawca w ramach dostarczonej infrastruktury zaimplementuje bezpieczne i szyfrowane mechanizmy dostępowe i udostępni konto Zamawiającemu w celu dokonania akceptacji parametrów technicznych i konfiguracji.
8. W ramach łączy VPN dostęp do zarządzalnych elementów infrastruktury musi zostać zabezpieczony szyfrowanym połączeniem.

14. Utrzymanie systemu

1. Wykonawca zobowiązany jest do utrzymania wszystkich dostarczonych elementów w ramach zamówienia.
2. Przez utrzymanie Zamawiający rozumie wszelkie prace, opłaty, koszty, operacje niezbędne do utrzymania w pełni funkcjonującego przedmiotu zamówienia.

3. W ramach utrzymania usługi Zamawiający zobowiązany jest do bieżącej aktualizacji wszelkich komponentów wykorzystanych do poprawnego funkcjonowania usługi.
4. W przypadku zmian prawnych w okresie utrzymania systemu Wykonawca zobowiązany jest do wprowadzenia wszelkich zmian, poprawek, zabezpieczeń wynikających ze zmienionych przepisów prawnych.
5. Utrzymanie systemu trwa przez cały okres gwarancji.

15. Warunki nieodpłatnej gwarancji

1. Wykonawca udziela Zamawiającemu nieodpłatną gwarancję jakości i funkcjonowania Systemu przez okres 12 miesięcy, a także zapewnia, że wykonane przez niego prace stanowiące przedmiot zamówienia zostały wykonane zgodnie z umową, specyfikacją techniczną oraz niezbędnymi uzgodnieniami, a także zgodnie z najlepszą wiedzą wykonawcy oraz aktualnie obowiązującymi zasadami wiedzy technicznej oraz obowiązującymi przepisami prawa, w tym istniejącymi w tym zakresie polskimi normami. Wykonawca jest zobowiązany zrealizować wszelkie świadczenia w ramach usługi gwarancyjnej w taki sposób, aby zapewnić pełną funkcjonalność Systemu w trakcie trwania nieodpłatnej gwarancji.
2. W okresie trwania gwarancji Wykonawca zobowiązuje się do zapewnienia prawidłowego funkcjonowania Systemu.
3. Wykonawca zobowiązany jest do usuwania Błędów w Czasie Naprawy.
4. Strony uzgadniają następujące zasady usuwania Błędów:
   1) Wykonawca zobowiązuje się dotrzymać następujących parametrów:

	Czas Reakcji	Czas Naprawy
Błąd Krytyczny	15 min	Do 6 godzin
Błąd Poważny	15 min	1 dzień roboczy
Błąd Niskiej Kategorii	15 min	5 dni roboczych

   2) Wykonawca zapewni przyjmowanie Zgłoszeń 5 dni w tygodniu godzinach 7.00-16.00.
   3) Czasy wskazane w tabeli powyżej liczone są od chwili dokonania zgłoszenia, w sposób ciągły.
5. Wykonawca zapewnia świadczenie usług gwarancyjnych, obejmujących:
   1) administrowanie środowiskiem produkcyjnym,
   2) monitorowanie działania Systemu,
   3) usuwania Błędów,
   4) dostarczanie aktualizacji i poprawek do Modułu Telerehabilitacji,
   5) aktualizację Modułu Telerehabilitacji w zakresie bezpieczeństwa aplikacji,
   6) weryfikacji Modułu Telerehabilitacji w zakresie poprawnego funkcjonowania po aktualizacjach systemów operacyjnych serwerów,
   7) weryfikacji i rekonfiguracji Modułu Telerehabilitacji w zakresie poprawnego funkcjonowania po aktualizacji komponentów systemu operacyjnego, bazy danych oraz innych niezbędnych do jego działania i wskazanych przez Wykonawcę w ramach architektury środowiska i systemów,
   8) aktualizacji Modułu Telerehabilitacji w zakresie zgodności z aktami prawnymi oraz wytycznymi organów państwowych w zakresie funkcjonowania Telerehabilitacji,
   9) aktualizacji i rekonfiguracji Modułu Telerehabilitacji w zakresie naprawy zgłoszonych usterek,
   10) zapewnienia wsparcia technicznego (na warunkach SLA) w zakresie zgłoszeń dotyczących obsługi oraz błędów w działaniu dla wszystkich użytkowników,
   11) zapewnienia wsparcia technicznego dla problemów użytkowników w wymiarze do 126 godzin,
   12) zapewnienia na bieżąco niezbędnych dla realizacji gwarancji wyjaśnień dla Zamawiającego w przypadku problemów z działaniem aplikacji,
   13) konsultowania i uzgadnianie prac serwisowych, konserwacyjnych oraz aktualizacyjnych z Zamawiającym,

14) zapewnienia aktualizacji Systemu gwarantujących poprawne działanie dla najnowszych komponentów systemowych dla infrastruktury oraz warstwy systemów operacyjnych i komponentów aplikacji,
15) Gwarancja obejmuje: nośniki elektroniczne, dokumentację techniczną dostarczoną wraz przedmiotem zamówienia oraz zgodność systemu z wymaganiami, wytycznymi które ma obowiązek spełnić,
16) zagwarantowanie ciągłości pracy Modułu poprzez potrzebne prace, opłaty, koszty, operacje niezbędne do utrzymania w pełni funkcjonującego przedmiotu zamówienia.

6. Wykonawca zobowiązuje się do zapewnienia ciągłości serwisu gwarancyjnego w wypadku zakończenia działalności swojego przedsiębiorstwa w czasie, na który została udzielona gwarancja.
7. Wykonawca gwarantuje, że Moduł Telerehabilitacji będzie działał zgodnie z jego opisem i instrukcjami.

16. System monitoringu infrastruktury Departamentu Cyfryzacji (zwany dalej SMDC)

1. Przedmiot zamówienia musi być podłączony do SMDC.
2. Podłączenie do SMDC musi być zrealizowane za pomocą:
   1) w przypadku maszyn wirtualnych lub serwerów fizycznych: za pomocą oprogramowania zabbix_agent2 (link: https://www.zabbix.com/download_agents);
   2) w przypadku innych urządzeń lub systemów, na których nie można zainstalować zabbix_agent2 należy włączyć protokół SNMP v3.
3. W konfiguracji oprogramowania zabbix_agent2 należy podać adres IP serwera monitorującego Zamawiającego. Należy uzupełnić pola „Server”, „ServerActive” oraz „Hostname”.
4. Konfigurację protokołu SNMP v3 należy uzgodnić z Zamawiającym, tj. klucze dostępowe, hasła, adresy IP.
5. W przypadku zmiany adresacji SMDC lub ustawień dla SNMP v3 Wykonawca zobowiązany jest do niezwłocznego wprowadzenia stosownych modyfikacji.
6. Adres IP serwera SMDC powinien być dodany do białej listy hostów komunikujących się z przedmiotem zamówienia.
7. Komunikacja między SMDC a Przedmiotem Zamówienia może następować tylko i wyłącznie po sieci lokalnej.