Znak Funduszy Europejskich (FE) 
złożony z symbolu graficznego, nazwy Fundusze Europejskie oraz nazwy programu, z którego w części lub w całości finansowany jest  projekt
Znak barw Rzeczypospolitej Polskiej (znak barw RP) 
złożony z barw RP oraz nazwy „Rzeczpospolita Polska”
Znak godło Województwa Świętokrzyskiego
Znak Unii Europejskiej (UE) 
złożony z flagi UE, napisu Unia Europejska i nazwy funduszu, który współfinansuje projekt 

**Załącznik nr 1B do SIWZ**

**Szczegółowy Opis Przedmiotu Zamówienia**

**Dostawa i Wdrożenie Infrastruktury Serwerowej i Sieciowej oraz oprogramowania dla Szpitalnego Systemu Informatycznego (SSI)**

**dla Zespołu Opieki Zdrowotnej we Włoszczowie**

**Szpital Powiatowy im. Jana Pawła II**

**dotyczy części 2 zamówienia**

Włoszczowa 2020

Spis treści

[Rozdział I. Założenia początkowe oraz wymagania ogólne 3](#_Toc29458802)

[I.1 Wprowadzenie 3](#_Toc29458803)

[I.2 Cel projektu 3](#_Toc29458804)

[I.3 Akty prawne 4](#_Toc29458805)

[I.4 Ogólny opis przedmiot zamówienia 4](#_Toc29458806)

[I.5 Termin realizacji Przedmiotu Zamówienia 6](#_Toc29458807)

[I.6 Organizacja wdrożenia 6](#_Toc29458808)

[I.6.1 Założenia podstawowe 6](#_Toc29458809)

[I.6.2 Przygotowanie Dokumentacji 7](#_Toc29458810)

[I.6.3 Harmonogram wdrożenia 7](#_Toc29458811)

[I.6.4 Dokumentacja Powykonawcza 7](#_Toc29458812)

[I.6.5 Odbiór Etapu/Dokumentacji/Końcowy 9](#_Toc29458813)

[I.6.6 Testy 9](#_Toc29458814)

[I.6.7 Dodatkowe zobowiązania Wykonawcy 9](#_Toc29458815)

[I.6.8 Instruktaże stanowiskowe 9](#_Toc29458816)

[Rozdział II. Szczegółowy opis przedmiotu zamówienia 11](#_Toc29458817)

[II.1 modernizacja sieci LAN w zakresie dostawy i wdrożenia aktywnych urządzeń sieciowych 11](#_Toc29458818)

[II.1.1 Przełącznik rdzeniowy 11](#_Toc29458819)

[II.1.2 Przełącznik dostępowy 14](#_Toc29458820)

[II.1.3 Wkładki SFP+ 15](#_Toc29458821)

[II.1.4 UTM 15](#_Toc29458822)

[Rozdział III. Gwarancja 21](#_Toc29458823)

[III.1.1 Usługi gwarancyjne 21](#_Toc29458824)

# Założenia początkowe oraz wymagania ogólne

## Wprowadzenie

W projekcie „Informatyzacja Placówek Medycznych Województwa Świętokrzyskiego (InPlaMed WŚ), w ramach Regionalnego Programu Operacyjnego Województwa Świętokrzyskiego na lata 2014-2020 (RPOWŚ 2007-2014)”, bierze udział Województwo Świętokrzyskie - będące Liderem Projektu, w imieniu którego zadania realizowane są przez Urząd Marszałkowski Województwa Świętokrzyskiego i 8 podmiotów leczniczych jednostek organizacyjnych Województwa oraz 12 podmiotów leczniczych będących jednostkami organizacyjnymi powiatów.

## Cel projektu

Głównym celem Projektu „Informatyzacja Placówek Medycznych Województwa Świętokrzyskiego” jest wdrożenie Elektronicznej Dokumentacji Medycznej (EDM) w placówkach medycznych objętych projektem, z zastosowaniem rozwiązań technologicznych i organizacyjnych zapewniających ciągłość działania oraz zgodność z regulacjami i wymogami prawnymi, protokołami przyjętymi w ochronie zdrowia, a także wytycznymi Centrum Systemów Informacyjnych Ochrony Zdrowia, jako instytucji państwowej, której zadaniem jest budowa oraz wspieranie i monitorowanie procesów budowy systemów informacyjnych w ochronie zdrowia. Cel ten przekłada się na usprawnienie zarządzania i podniesienie jakości procesów leczniczych.

Ponadto zakłada się budowę usług elektronicznych w obszarze ochrony zdrowia, świadczonych w ramach poszczególnych placówek medycznych biorących udział w projekcie oraz całego regionu, na rzecz pacjentów oraz personelu medycznego, w jak najszerszym możliwym do realizacji pod względem finansowym, organizacyjnym i prawnym zakresie.

Kluczową usługą budowaną w ramach Projektu będzie gromadzenie i udostępnianie elektronicznej dokumentacji medycznej (EDM) w sposób zapewniający nienaruszalność i bezpieczeństwo przechowywania danych w długim okresie czasu, przy jednoczesnym zapewnieniu łatwego dostępu dla wszystkich uprawnionych użytkowników oraz zachowaniu wysokiej wydajności działania.

Zakłada się osiągnięcie celów Projektu poprzez rozbudowę i rozszerzenie aktualnego stanu informatyzacji poszczególnych placówek medycznych uczestniczących w projekcie z możliwością w przyszłości rozbudowy o kolejne e-usługi i funkcjonalności, w tym także budowę integracyjnej warstwy regionalnej.

Zakres rozbudowy i rozszerzenia aktualnego stanu informatyzacji poszczególnych placówek medycznych został w ramach projektu zaktualizowany indywidualnie dla poszczególnych placówek medycznych uczestniczących w projekcie na podstawie analizy stanu aktualnego. W ramach projektu zakładane jest - w zależności od indywidualnych potrzeb placówek medycznych - zarówno dostarczenie wymaganych w ramach projektu funkcjonalności biznesowych realizowanych poprzez dostawę nowych systemów dziedzinowych (lub dostosowanie i integrację zastanych medycznych systemów dziedzinowych) oraz lokalnych repozytoriów EDM. Przewidywana jest także rozbudowa warstwy infrastrukturalno–systemowej poprzez dostawę komponentów i rozwiązań w obszarze sieciowym, sprzętowym oraz oprogramowania systemowego.

## Akty prawne

Dostarczone rozwiązania teleinformatyczne, ze szczególnym uwzględnieniem dostarczanego i wdrażanego Oprogramowania, muszą być zgodne z powszechnie obowiązującymi przepisami prawa polskiego i europejskiego. Rozwiązania muszą pozwalać na gromadzenie, przetwarzanie i analizowanie danych i informacji w obszarach objętych wdrożeniem.

## Ogólny opis przedmiot zamówienia

**Część 2** – **modernizacja sieci LAN w zakresie dostawy i wdrożenia sieciowej infrastruktury sprzętowej w postaci urządzeń aktywnych.**

1. Przedmiot zamówienia niniejszego postepowania przetargowego dla części 2 obejmuje:
2. **modernizacja sieci LAN** w zakresie dostawy i wdrożenia sieciowej infrastruktury sprzętowej:

|  |  |  |
| --- | --- | --- |
| **Poz. SOPZ** | **Opis** | **Ilość** |
| **Rozdział II.1** | **Modernizacja sieci LAN** |  |
| **AKTYWNE URZĄDZENIA SIECIOWE** | | |
| II.1.1 | Przełącznik rdzeniowy | 2 szt. |
| II.1.2 | Przełącznik dostępowy | 9 szt. |
| II.1.3 | Wkładki SFP+ | 30 szt. |
| II.1.4 | UTM | 1kpl/2 szt. |

1. Przedmiot zamówienia musi być dostarczany, wdrożony i zainstalowany w całości do siedziby Zamawiającego.
2. Wszystkie dostarczane:

* Produkty (rozumiane jako elementarny efekt działań/prac/dostaw objętych całym zakresem Przedmiotu Zamówienia wykonywanych przez Wykonawcę podczas realizacji Umowy   
  w poszczególnych Etapach).
* Komponenty (rozumiane jako integralna część dostawy i wdrożenia Przedmiotu Zamówienia, składający się przynajmniej z jednego Produktu lub wielu Produktów powiązanych ze sobą merytorycznie) podlegają usługom projektowania, dostaw, instalacji, konfiguracji i wdrożenia.

1. Usługi projektowania, instalacji, konfiguracji i wdrożenia Wykonawca przeprowadzi zgodnie   
   z zapisami SOPZ dla część 2 w uzgodnieniu z Zamawiającym zgodnie z obowiązującymi przepisami, zasadami wykonywania projektów teleinformatycznych oraz najlepszymi praktykami w ich realizacji.
2. Wykonawca jest zobowiązany do realizacji Przedmiotu Zamówienia zgodnie z zasadami i wytycznymi Zamawiającego, niniejszymi zapisami SOPZ oraz Umowy.
3. Ilekroć w niniejszym SOPZ Zamawiający użył w opisie oznaczeń norm, aprobat, specyfikacji technicznych i systemów odniesienia, o których mowa w art. 30 ust. 1-3 Pzp należy je rozumieć jako przykładowe. Zamawiający zgodnie z art. 30 ust. 4 ustawy Pzp dopuszcza produkty równoważne opisywanym w treści SIWZ. Jeżeli zapisy zawarte w niniejszym dokumencie wskazywałyby w odniesieniu do rozwiązań, materiałów lub urządzeń znaki towarowe lub pochodzenie Zamawiający, zgodnie z art. 29 ust. 3 ustawy PZP, dopuszcza składanie ofert na „produkty” równoważne. Wszelkie „produkty” pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, jakim musi odpowiadać produkt, aby spełnić wymagania stawiane przez Zamawiającego i stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia. Poprzez zapis dot. minimalnych wymagań parametrów jakościowych Zamawiający rozumie wymagania materiałów, sprzętu i urządzeń zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Tak więc posługiwanie się nazwami producentów /produktów/ ma wyłącznie charakter przykładowy. Zamawiający, przy opisie przedmiotu zamówienia, wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych, co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych parametrach lub lepszych. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, wykazujących spełnienie przez produkty równoważne ww. parametrów i cech.
4. Wykonawca musi dostarczyć wszelkie urządzenia i elementy, które są niezbędne do prawidłowego funkcjonowania całości. W przypadku, gdy w trakcie realizacji Przedmiotu Zamówienia okaże się, że brakuje jakiegokolwiek urządzenia i/lub elementu, którego brak spowoduje nieprawidłowe funkcjonowanie całości Przedmiotu Zamówienia, Wykonawca dostarczy je na własny koszt.
5. Zamawiający wymaga, aby zaoferowane rozwiązanie (system) było rozwiązaniem istniejącym, działającym, gotowym do wdrożenia i zapewniającym realizację wszystkich wymaganych w SIWZ   
   (w szczególności SOPZ) funkcjonalności na dzień składania ofert i nie może być w fazie opracowywania, budowy, testów, projektowania itp.
6. Wszelkie dostarczane urządzenia:

* Muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta   
  i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych.
* Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta.
* Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta.
* Urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
* Urządzenia muszą być dostarczone Zamawiającemu wraz z oryginalnymi opakowaniach producenta.
* Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji w dla użytkownika w języku polskim w formie papierowej lub elektronicznej.

## Termin realizacji Przedmiotu Zamówienia

1. Termin realizacji całości Przedmiotu zamówienia dla Części 2 wynosi **90 dni** od dnia zawarcia Umowy.

## Organizacja wdrożenia

### Założenia podstawowe

1. Przedmiot Zamówienia będzie realizowany w oparciu o zdefiniowany uprzednio przez Wykonawcę   
   i zaakceptowany Harmonogram wdrożenia, który powinien być uzgodniony i zaakceptowany przez Zamawiającego oraz odpowiednio utrzymywany w toku realizacji Przedmiotu Zamówienia.
2. Wykonawca w Harmonogramie wdrożenia musi uwzględnić w szczególności podział na zadania takie jak projektowanie, dostawy, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory.
3. Wykonawca umożliwi Zamawiającemu udział we wszystkich pracach realizowanych przez Wykonawcę w ramach realizacji Przedmiotu Zamówienia (m.in. w czasie projektowania, dostawach, instalacji/budowie, konfiguracji i wdrożeniu i testowaniu).
4. Wykonawca zobowiązany jest przeprowadzić dostawy Przedmiotu Zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym.
5. W przypadku dostarczania Infrastruktury Sprzętowej UTM i przełączników musi być ona oznakowana w taki sposób, aby możliwa była identyfikacja systemowa zarówno produktu jak i producenta, pochodzić z oficjalnych kanałów dystrybucji producentów i dostarczony w oryginalnych opakowaniach fabrycznych.
6. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie Przedmiotu Zamówienia.
7. Realizacja przedmiotu zamówienia będzie realizowana w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy.
8. Wykonawca zorganizuje prace tak, aby w maksymalnym stopniu nie zakłócać ciągłości funkcjonowania prac u Zamawiającego.
9. Obiekty podlegające inwestycji (obiekty służby zdrowia w których świadczone są usługi medyczne) są użytkowane w trybie ciągłym w czasie godzin pracy przez cały okres wykonywania Przedmiotu Zamówienia, co może powodować utrudnienia w miejscu prowadzenia prac. Nie ma możliwości całkowitego wyłączenia i zamknięcia w/w obiektów lub ich części na czas realizacji Przedmiotu Zamówienia. Poszczególne prace będą realizowane etapowo, tak aby zachować ciągłość świadczenia usług medycznych.
10. Wykonawca musi uwzględnić, że wszystkie prace wykonywane będą w użytkowanych obiektach przy dużym ruchu pracowników i chorych, tzn. organizacja prac powinna przede wszystkim zapewniać bezpieczeństwo przebywających w oddziałach pracowników i chorych oraz zachowanie ciszy nocnej w godzinach właściwych dla Zamawiającego.

### Przygotowanie Dokumentacji

1. W ramach procesu prac Wykonawca opracuje dla Zamawiającego Dokumentacje Przedmiotu Zamówienia(zwaną dalej Dokumentacja, Dokumentacja PZ), która składa się z nw. zakresów:
2. Harmonogram Wdrożenia.
3. Dokumentacja Powykonawcza.
4. Dokumentacja będzie zawierać bazowe zapisy opisujące budowane rozwiązania, procesy oraz sposób organizacji prac i wdrożenia. Na podstawie zapisów w Dokumentacji będą prowadzone   
   i odbierane poszczególne etapy realizowane w ramach Przedmiotu zamówienia.
5. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja Harmonogramu wdrożenia warunkuje rozpoczęcie prac Wykonawcy.
6. Harmonogram wdrożenia zostanie opracowane w oparciu o wymagania określone w niniejszym SOPZ dla części 2.

### Harmonogram wdrożenia

Wykonawca zobowiązany jest opracować na podstawie SIWZ wraz z załącznikami, szczegółowy harmonogram wdrożenia. Harmonogram należy przedstawić Zamawiającemu w terminie do 14 dni od podpisania Umowy.

### Dokumentacja Powykonawcza

1. Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powykonawczej obejmującej dokumentację użytkową, techniczną i eksploatacyjną. Dokumentacja Powykonawcza musi być dostarczona w języku polskim, w wersji elektronicznej w formacie edytowalnym oraz w co najmniej jednym egzemplarzu papierowym.
2. W dokumentacji muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację rozwiązań.
3. W szczególności dokumentacja ta powinna zawierać:

#### Wymogi ogólne:

1. Konfiguracja musi obejmować wszystkie urządzenia wdrożone, zainstalowane w ramach dostawy.
2. Przykładowy zestaw wymaganych danych konfiguracyjnych obejmuje:

* sieć (adresacja IP, itp.),

1. Opis architektury logicznej:

* schemat i opis powiązań logicznych poszczególnych komponentów i ich rolę w architekturze.

1. Procedury lub instrukcje instalacji, reinstalacji oraz aktualizacji.

* szczegółowy opis postępowania w przypadku tworzenia lub zmian w środowisku; jeśli wykorzystywane są procedury innych dostawców (dla standardowych komponentów wystarczy wskazać w dokumentacji szczegółowe odniesienie do procedur standardowych właściwych dla tych komponentów).

1. Procedury standardowe:

* opis możliwości stosowania standardowych procedur poprawnej eksploatacji dla rozwiązań wspierających (sprzętowych lub aplikacyjnych).

1. Dokumentacja procesu parametryzacji:

* wyszczególnienie wszystkich parametryzowanych elementów systemu wraz z opisem ich znaczenia i dopuszczalnych wartości oraz stosowanych wartości domyślnych.

1. Dokumenty z testów:

* Plan testów, scenariusze testowe i protokoły z testów akceptacyjnych.

1. Instrukcje obsługi i instrukcje użytkowania dla wersji dostarczonego oprogramowania.
2. Wkład do Polityki bezpieczeństwa w zakresie wdrożonego Systemu oraz Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych opracowane zgodnie   
   z wymaganiami określonymi w R[ozporządzeniu 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 (ogólne rozporządzenie o ochronie danych)](https://uodo.gov.pl/pl/131/224). Wkład do Polityki Bezpieczeństwa będzie zawierać w szczególności:

* opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

#### 2) Wymagania szczegółowe:

Dokumentacja powykonawcza logicznej struktury sieci powinna zawierać co najmniej:

|  |
| --- |
| **Dokumentacja Powykonawcza logicznej struktury sieci** |
| * Informacje ogólne |
| * Opis sposobu i struktury adresacji logicznej sieci |
| * Ogólny schemat logicznej struktury sieci |

### Odbiór Etapu/Dokumentacji/Końcowy

1. Odbiór Przedmiotu Zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy, w tym odebrania wszystkich Komponentów i Etapów oraz dostarczenia wymaganej zamówieniem Dokumentacji.
2. Odbiory będą odbywać się zgodnie z zapisami w Umowie stanowiącej Dodatek nr 4B do SIWZ.

### Testy

1. W ramach postepowania zostaną przeprowadzone wszystkie testy opisane w Dokumentacji. Celem testów jest weryfikacja przez Zamawiającego czy wszystkie prace wykonane w trakcie realizacji Przedmiotu Zamówienia zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy współudziale Zamawiającego jak i wskazanych przez Zamawiającego osób lub podmiotów zewnętrznych.
2. Pozytywne zakończenie testów wraz z usunięciem wskazanych Wad jest niezbędne, aby dla poszczególnych Komponentów oraz całego Przedmiotu Zamówienia dokonać odbioru końcowego.
3. Zamawiający ma prawo do weryfikacji należytego wykonania Umowy dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. W szczególności uzgodnienie określonych scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami i scenariuszami.
4. W przypadku zidentyfikowania Błędów lub Wad Wykonawca jest zobowiązany do ich poprawy przed odbiorem końcowym Przedmiotu Zamówienia.

### Dodatkowe zobowiązania Wykonawcy

1. Wykonanie Przedmiotu Zamówienia z efektywnością oraz zgodnie z praktyką i wiedzą zawodową.
2. Wykonanie w całości Przedmiotu Zamówienia w zakresie określonym w Umowie będącej Dodatkiem nr 4B do SIWZ.
3. Dokonanie z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres   
   i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającymi na każdym etapie realizacji.
4. Stosowanie się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego.
5. Udzielanie na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.
6. Współdziałanie z osobami wskazanymi przez Zamawiającego.

### Instruktaże stanowiskowe

1. Wykonawca zaplanuje w uzgodnieniu z Zamawiającym i przeprowadzi instruktaże stanowiskowe dla wskazanych przez Zamawiającego administratorów (2 osoby) w łącznym wymiarze nie mniej niż 20 osobogodzin.
2. Podczas instruktaży musi zostać przekazana niezbędna wiedza w zakresie umożliwiającym samodzielne administrowanie urządzeniami, w tym co najmniej aktualizacji firmware, konfiguracji urządzeń UTM i przełączników w zakresie funkcjonalności wskazanych w SOPZ.
3. Instruktaże stanowiskowe zostaną przeprowadzone w miejscu instalacji Przedmiotu Zamówienia. W przypadku potrzeby Zamawiający zapewni we własnym zakresie pomieszczenie dla przeprowadzenia instruktaży stanowiskowych.

# Szczegółowy opis przedmiotu zamówienia

## Modernizacja sieci LAN w zakresie dostawy i wdrożenia aktywnych urządzeń sieciowych

1. W ramach budowy sieci LAN, Wykonawca dostarczy aktywne urządzenia sieciowe   
   o minimalnych parametrach opisanych poniżej.
2. Sprzęt musi pochodzić z autoryzowanego przez jego producenta kanału dystrybucji w UE   
   i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim.
3. Wszystkie urządzenia muszą być fabrycznie nowe.

### Przełącznik rdzeniowy

Wymagane dostarczenie 2 szt. przełączników spełniających poniżej opisane minimalne parametry funkcjonalne:

|  |  |
| --- | --- |
| **Cecha** | **Wymagania minimalne** |
| 1. Obudowa | Obudowa umożliwiająca montaż w szafie RACK 19”, wysokość maksymalnie 1U, głębokość nie przekraczająca 46cm |
| 2. Porty | * Minimum 40 portów 1G/10GbE SFP+ umieszczonych z przodu obudowy * Minimum 2 porty 40GbE QSFP+ umieszczone z przodu obudowy * Dedykowany port Ethernet do zarządzania poza pasmem - out of band management * Port konsoli RS232 ze złączem DB9 lub RJ45 * Port USB 2.0 |
| 3. Warstwa przełączania | Przełączanie w warstwie 2 i 3 modelu OSI |
| 4. Przepustowość | Minimum 713 Mpps dla pakietów 64 bajtowych |
| 5. Wydajność | Minimum 960 Gbps (prędkość przełączania „wirespeed” dla każdego portu przełącznika) |
| 6. Tablica adresów MAC | Minimum 64000 pozycji |
| 7. Routing | Routing IPv4 – statyczny i dynamiczny (min. RIP, IS-IS, OSPF, BGP)  Routing IPv6 – statyczny i dynamiczny (min. RIPng, IS-ISv6, OSPFv3) Tablica routingu o pojemności co najmniej 1000 wpisów |
| 8. Pamięć | * Minimum 512MB pamięci typu Flash * Minimum 2GB pamięci operacyjnej |
| 8. Funkcje stackowania | Funkcja łączenia w stos grupy przełączników, urządzenia połączone w stos widziane jako jedno logiczne urządzenie ze wspólnym zarządzaniem. Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 360 portów 10GbE SFP+. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain)).  Łączenie w stos z wykorzystaniem portów 10Gb, 40Gb i agregowanych portów 10Gb (w celu zwiększenia przepustowości w stosie) Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie |
| 9. Bufor pakietów | Wielkość bufora pakietów: minimum 9MB |
| 10. Ramki Jumbo | Obsługa ramek Jumbo o wielkości 10kB |
| 11. Zarządzanie i monitorowanie | * Obsługa funkcji logowania do sieci („Network Login”) zgodna ze standardem IEEE 802.1x * Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS * Zarządzanie poprzez port konsoli, SNMP v.1, 2c i 3, Telnet, SSH v.2 * Syslog |
| 12.Obsługa mechanizmów | Strict priority (SP) queuing, weighted fair queuing (WFQ), weighted random early discard (WRED), weighted deficit round robin (WDRR), explicit congestion notification (ECN), SP+WFQ oraz SP+WDRR. |
| 13. Wentylacja | Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa niezależne moduły wentylatorów) |
| 14. Pozostałe funkcje | 1. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol 2. Obsługa sieci IEEE 802.1Q VLAN – 4094 sieci VLAN oraz IEEE 802.1ad QinQ 3. Obsługa IGMP Snooping v1/v2/v3, PIM Snooping, MLD snooping v1/v2 oraz IPv6 PIM Snooping 4. Wsparcie dla FibreChannel over Ethernet (FCF/Transit/NPV) 5. Wsparcie dla Data Center Bridging (DCB):    * IEEE 802.1Qbb Priority Flow Control (PFC)    * Data Center Bridging Exchange (DCBX) 6. Obsługa Transparent Interconnection of Lots of Links (TRILL) 7. Obsługa ECMP (Equal Cost Multi Path) 8. Serwer DHCP, klient DHCP, obsługa opcji 82 (snooping i relay), DHCP snooping 9. Obsługa list ACL na bazie informacji z warstw 3/4 modelu OSI.   Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia   1. Obsługa standardu 802.1p 2. Możliwość zmiany wartości pola DSCP i/lub wartości priorytetu 802.1p 3. Funkcje mirroringu: 1 to 1 Port mirroring, Many to 1 port mirroring, remote mirroring 4. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) oraz LLDP-MED 5. Obsługa sFlow 6. Obsługa NETCONF 7. Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3 8. Obsługa Network Time Protocol (NTP), Simple Network Time Protocol (SNTP) oraz kompatybilność z Precision Time Protocol (PTP) RFC 1855 9. Obsługa OAM (IEEE 802.3ah) 10. Obsługa CFD (IEEE 802.1ag) 11. Modularny system operacyjny ze wsparciem dla In Services Software Upgrade (ISSU) i skryptów w języku Python 12. Obsługa Quality of Service |
| 15. Administracja | 1. Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania). Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji). 2. Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian. |
| 16. Pobór mocy | Maksymalny pobór mocy nie większy niż 180W |
| 17. Środowisko pracy | Minimalny zakres temperatur pracy od 0°C do 45°C |
| 18. Akcesoria | Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia.  Należy dostarczyć 2 wkładki QSFP+, 40 Gb SR, Optical Transceiver lub dostarczyć dwie sztuki kabli QSFP+ to QSFP+ 40GbE do łączenia bezpośredniego o długości min. 1m. |

### Przełącznik dostępowy

Wymagane dostarczenie 9 szt. przełączników spełniających poniżej opisane minimalne parametry funkcjonalne:

|  |  |
| --- | --- |
| **Cecha** | **Wymagania minimalne** |
| 1. Obudowa | Obudowa umożliwiająca montaż w szafie RACK 19”, wysokość maksymalnie 1U, głębokość nie przekraczająca 31 cm |
| 2. Porty | -Minimum 48 portów gigabitowych w standardzie 100/1000BaseT -Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP). |
| 3. Przepustowość | minimum 175 Gb/s |
| 4. Wydajność | minimum 110 Mp/s |
| 5. Tablica adresów MAC | Tablica adresów MAC o wielkości minimum 32000 pozycji |
| 6. Routing | Routing IPv4 – minimum: statyczny, RIPv2, OSPF  Routing IPv6 – minimum: statyczny, RIPng, OSPFv3  Wielkość tablicy routingu: minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6 |
| 7. Pamięć i procesor | Procesor minimum dwurdzeniowy 1000MHz, 1GB DDR3 SDRAM, |
| 8. Funkcje stackowania | Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 4 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster).  Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie |
| 9. Bufor pakietów | Minimum 12 MB |
| 10. Ramki Jumbo | Obsługa Ramek Jumbo. |
| 11. Zarządzanie i monitorowanie | Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https, Syslog |
| 12. Obsługa standardów i protokołów | Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping, VxLAN, IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol, Obsługa 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLAN, Funkcja Root Guard oraz BPDU protection, Wsparcie dla funkcji DHCP server, DHCP Relay, Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI |
| 13. Administracja | Musi być możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku.  Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej |
| 14. Pobór mocy | Maksymalny pobór mocy nie większy niż 70W |
| 15. Środowisko pracy | Minimalny zakres pracy od 0°C do 45°C |

### Wkładki SFP+

Wymagane dostarczenie 30 szt. wkładek spełniających poniżej opisane minimalne parametry funkcjonalne:

|  |  |
| --- | --- |
| **Cecha** | **Wymagania minimalne** |
| 1. Typ | Zamawiający wymaga dostarczenia wkładki SFP+ 10Gb SR kompatybilnych z przełącznikami z pozycji pkt. II.1.1, II.1.2 wraz z kablem LC-LC min. 5 metrów. |

### UTM

1. Wymagane dostarczenie 2 szt. urządzeń UTM (1 kpl) spełniających poniżej opisane minimalne parametry funkcjonalne.
2. Ze względu na charakter działalności jaką prowadzi Zamawiający (świadczenie usług medycznych 24/7/365) Wykonawca zobowiązany jest, w ramach wykonania przedmiotu umowy, do zminimalizowania przerwy w działaniu infrastruktury sieciowej szpitala działającej w oparciu o urządzenia UTM. W tym celu ewentualne przerwy związane z wdrożeniem dostarczonego rozwiązania nie przekroczą łącznie 30 minut a czas i termin zostanie ustalony z Zamawiającym.
3. W ramach realizacji zamówienia Wykonawca dostarczy, skonfiguruje, wdroży i uruchomi zaporę ogniową co najmniej w zakresie:

* Wniesienia, ustawienia i fizycznego montażu zapory ogniowej w miejscu wskazanym przez Zamawiającego.
* Podłączenia zapory ogniowej do infrastruktury Zamawiającego z uwzględnieniem specyfiki sieci Zamawiającego.
* Wykonania procedury aktualizacji firmware dostarczonej zapory ogniowej do najnowszej wersji oferowanej przez producenta sprzętu.
* Zaadresowanie zapory ogniowej zgodnie z przydzielonymi przez administratorów Zamawiającego adresami IP.
* Konfiguracja klastra HA wraz z rozszyciem łączy WAN.
* Konfiguracja routing na zaporze zgodnie z zaleceniami administratorów Zamawiającego.
* Konfiguracja podsieci LAN zgodnie z zaleceniami administratorów Zamawiającego.
* Konfiguracja VLAN na dostarczonych urządzeniach zgodnie z zaleceniami administratorów Zamawiającego.
* Należy skonfigurować polityki bezpieczeństwa dostarczone w ramach zakupionych licencji (IPS, antywirus, web filtering), VPN, DMZ, NAT zgodnie z tzw. Best-practices oraz zaleceniami Zamawiającego.
* Należy skonfigurować dostęp do urządzeń SSH oraz HTTPS.

|  |  |
| --- | --- |
| **Cecha** | **Wymagania minimalne** |
| 1. Wymagane podstawowe funkcje | 1. Zapora sieciowa typu Next Generation Firewall (NGFW) 2. Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku. 3. Minimalna ilość interfejsów:    1. 2 interfejsy 10 GbE SFP+    2. 8 interfejsy 2.5 GbE SFP    3. 4 interfejsy 2.5 GbE    4. 12 interfejsów RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa.    5. 2 interfejsy USB dla przyszłych potrzeb i do podłączenia modemu 3G    6. 1 interfejs konsoli do zarządzania zaporą    7. 1 interfejs RJ-45 Ethernet 10/100/1000 do zarządzania zaporą 4. Zapora powinna posiadać dysk SSD o pojemności przynajmniej 32 GB z możliwością wymiany na większy. 5. Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa 6. Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji 7. Możliwość utworzenia przynajmniej 256 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q 8. Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej 9. Minimalna ilość jednocześnie obsługiwanych połączeń: 2 000 000 10. Możliwość obsłużenia przynajmniej 14 000 nowych połączeń w ciągu 1 sekundy. 11. Przepustowość urządzenia pracującego w trybie stateful firewall: 3,75 Gbps – dla ramki 1518B zgodnie z RFC 2544 12. Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 1.8 Gbps 13. Przepustowość urządzenia pracującego jako koncentrator VPN: 1.5 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544 14. Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń, jeśli chodzi o wielkość skanowanych plików) – 730 Mbps 15. Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 3 000 16. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 500 z możliwością rozszerzenia do przynajmniej 3 000. 17. Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne. 18. Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 300 Mbps oraz obsłużyć 24 000 połączeń. 19. Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP 20. Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site) 21. Wsparcie funkcjonalności IP Helper lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa) 22. Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP 23. Wsparcie dla Dynamicznego DNS tzw. DDNS 24. Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne. 25. Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony, na które użytkownik wchodzi bezpośrednio). 26. Administrator powinien mieć możliwość tworzenia różnych akcji, dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak:     1. wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron)     2. wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony     3. wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki. 27. Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps 28. Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL. 29. Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci. 30. Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego. 31. Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN) 32. Kontrola dostępności zestawionych tuneli VPN 33. Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP. 34. Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty. 35. Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić) 36. Funkcja NAT oparta o reguły bezpieczeństwa. 37. NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe) 38. Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych. 39. Zintegrowany system skanowania antyspyware 40. Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www. 41. System IPS musi używać algorytmu szeregowego przetwarzania. 42. Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex). 43. Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji     1. Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie.     2. Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur     3. Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur. 44. System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików. 45. Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa 46. Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi 47. Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p 48. Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń 49. Urządzenie powinno mieć możliwość analizy behawioralnej (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minimum 3 silników pochodzących od różnych producentów w celu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkich silnikach. Licencja na tą funkcjonalność nie jest przedmiotem przetargu, ale urządzenie powinno zapewniać taką funkcjonalność w celu późniejszej rozbudowy systemu. 50. Wymagane jest dostarczenie dodatkowego urządzenia pełniącego funkcję standby w klastrze wysokiej dostępności (HA) z urządzeniem podstawowym. Urządzenie standby powinno mieć identyczne parametry wydajnościowe jak podstawowa jednostka. |
| 2. Licencjonowanie | 1. Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji oraz zapewnienie wsparcia technicznego 24x7 na okres 5 lat.  2. Licencja na oprogramowanie służące do przechowywania logów z systemu firewall i generowania na ich podstawie raportów. Wymagana jest licencja, która pozwoli na korzystanie z oprogramowania przez okres 60 miesięcy. |
| 3. Akcesoria | Zamawiający wymaga dostarczenia wraz z firewallem:  - 4 x Transceiver 10GBASE-SR;  - 4 x kabel LC-LC min. 5 metrów; |

# 

# Gwarancja

1. Wykonawca w ramach realizacji Przedmiotu Zamówienia udzieli Zamawiającemu gwarancji jakości (dalej zwanej „gwarancją”) na niniejszy przedmiot zamówienia:
2. **modernizacja sieci LAN** w zakresie dostawy i wdrożenia Infrastruktury aktywnej sieci

|  |  |  |
| --- | --- | --- |
| **Poz. SOPZ** | **Opis** | **Okres gwarancji (minimalny)** |
| **AKTYWNE URZĄDZENIA SIECIOWE** | | |
| II.1.1 | Przełącznik rdzeniowy | 60 miesięcy gwarancji producenta obejmująca wszystkie elementy przełącznika  (również zasilacze i wentylatory) |
| II.1.2 | Przełącznik dostępowy | 60 miesięcy gwarancji producenta obejmująca wszystkie elementy przełącznika  (również zasilacze i wentylatory) |
| II.1.3 | Wkładki SFP+ | 60 miesięcy gwarancji producenta obejmująca wszystkie elementy przełącznika  (również zasilacze i wentylatory) |
| II.1.4 | UTM | 60 miesięcy gwarancji producenta  Obejmująca również licencje  dla wszystkich funkcji bezpieczeństwa |

1. Bieg terminów gwarancji określonych w ust. 1 będą rozpoczynać się z dniem podpisania Protokołu Odbioru Końcowego bez uwag przez Zamawiającego.
2. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzeń oraz wsparcia technicznego.

### Usługi gwarancyjne

1. W okresie gwarancji Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu rozumianych jako Awaria lub Usterka zgodnie z definicjami jak poniżej:
2. **Awaria -** Kategoria Wady w Infrastrukturze Sprzętowej powodująca brak działania lub niepoprawne działanie Przedmiotu Zamówienia u Zamawiającego, uniemożliwiające jego użytkowanie. Sytuacja, w której rozwiązanie w ogóle nie funkcjonuje lub nie jest możliwe realizowanie istotnych funkcjonalności Komponentów/Produktów Przedmiotu Zamówienia.
3. **Usterka -** Należy przez to rozumieć kategorię Wady w Infrastrukturze Sprzętowej oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz SOPZ, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi Zamawiającego.
4. Przyjęcie zgłoszenia Wady przez Wykonawcę, odbywać się będzie w okresie dostępności Wykonawcy wskazany w Tabeli 1, w zależności od tego czego wada dotyczy, poprzez dostępny on-line System Zgłaszania i przyjmowania uwag oraz Wad (dalej zwany „SZ”) przy czym:
5. System Zgłoszeń dostarczy Wykonawca (będzie on utrzymywany i administrowany przez Wykonawcę), wpis zgłoszenia do SZ będzie dokonywał Zamawiający,
6. za skuteczne przyjęcie zgłoszenia Wady uważa się będzie wprowadzenie przez Zamawiającego wpisu do SZ zawierającego opis zgłaszanej Wady i termin jej zgłoszenia. W razie trudności   
   z dostępem on-line do SZ, zgłoszenia Wady mogą odbywać się także telefonicznie pod ustalonym numerem telefonu lub pisemnie na formularzu przesyłanym na ustalony adres e-mail, opcjonalnie faksem, których numery i adresy zostaną podane przez Wykonawcę w. terminie 15 dni roboczych od dnia podpisania Umowy wraz ze wzorem formularza zgłoszenia Wady.
7. Gwarancja musi zapewniać wymianę uszkodzonego sprzętu, kabli i elementów oraz zapewniać dostęp do aktualizacji oprogramowania, bez wiedzy i wsparcia technicznego producenta.
8. W ramach gwarancji Wykonawca będzie świadczył następujące usługi:
9. Usuwanie Wad w dostarczonym Przedmiocie Zamówienia w przypadku stwierdzenia przez Zamawiającego Wady w jego działaniu, w terminach określonych poniżej:

**Tabela 1 Usługi gwarancji aktywnych urządzeń sieciowych**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **KWALIFIKACJA ZGŁOSZENIA WADY** | **OKRES DOSTĘPNOŚCI WYKONAWCY** | **ROZWIĄZANIE  ZASTĘPCZE\*** | **CZAS REAKCJI WYKONAWCY** | **CZAS NAPRAWY** |
| AWARIA | 24/7/365 | niezwłocznie, nie później niż 24 godzin od czasu przyjęcia zgłoszenia | niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia | niezwłocznie, nie później  niż 14 dni od czasu przyjęcia zgłoszenia |
| USTERKA | nie dotyczy | niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia | niezwłocznie nie później niż 30 dni od dnia przyjęcia zgłoszenia |

\*nie dotyczy sprzętu zastępczego

1. dopuszcza się zmianę kwalifikacji zgłoszenia Wady, po uprzedniej zgodzie Zamawiającego. Do czasu potwierdzenia zmiany kwalifikacji, uznaje się za obowiązującą kwalifikację pierwotną,
2. czasy naprawy mogą być inne niż wskazane w powyższej tabeli, jeżeli Zamawiający zaakceptuje zmianę kwalifikacji zgłoszenia, o której mowa w punkcie 2),
3. w przypadku braku możliwości usunięcia Wady lub przedstawienia rozwiązania zastępczego zdalnie, Wykonawca zobowiązany jest do świadczenia gwarancji bezpośrednio w lokalizacji Zamawiającego,
4. Wykonawca w okresie trwania gwarancji, do 5 dnia każdego miesiąca, przedstawi Zamawiającemu raport zawierający co najmniej: numer zgłoszenia, kwalifikację zgłoszenia, godzinę i datę zgłoszenia, temat zgłoszenia, status zgłoszenia, godzinę i datę usunięcia Wady, czas naprawy,

Uwaga:

W przypadku zapisu terminu jako:

* Dzień Roboczy należy rozumieć każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
* Godziny Robocze należy rozumieć godziny od 8.00 do 16.00 w każdym Dniu Roboczym.

W innych przypadkach należy rozumieć jako dzień kalendarzowy.