Fundusze Europejskie Program Regionalny | Rzeczpospolita Polska | Województwo Świętokrzyskie | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Załącznik nr 1B do SIWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa i Wdrożenie Infrastruktury Serwerowej i Sieciowej oraz oprogramowania dla Medycznego Systemu Informatycznego (MSI)

DLA WOJEWÓDZKIEGO OŚRODKA MEDYCYNY PRACY W KIELCACH

DOTYCZY CZĘŚCI 2 ZAMÓWIENIA

Kielce 2020

ROZDZIAŁ I. ZAŁOŻENIA POCZĄTKOWE ORAZ WYMAGANIA OGÓLNE 3

I.1 WPROWADZENIE 3
I.2 CEL PROJEKTU 3
I.3 AKTY PRAWNE 4
I.4 OPIS PRZEDMIOTU ZAMÓWIENIA 4
I.5 TERMIN REALIZACJI PRZEDMIOTU ZAMÓWIENIA 6
I.6 ORGANIZACJA WDROŻENIA 6
I.6.1 Założenia podstawowe 6
I.6.2 Przygotowanie Dokumentacji 7
I.6.3 Harmonogram wdrożenia 7
I.6.4 Dokumentacja Powykonawcza 7
I.6.5 Odbiór Etapu/Dokumentacji/Końcowy 8
I.6.6 Testy 8
I.6.7 Dodatkowe zobowiązania Wykonawcy 9
I.6.8 Instruktaże stanowiskowe 9

ROZDZIAŁ II. SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA 9

II.1 MODERNIZACJA SIECI LAN W ZAKRESIE DOSTAWY I WDROŻENIA AKTYWNYCH URZĄDZEŃ SIECIOWYCH 9
II.1.1 Przełącznik LAN 10
II.1.2 Przełącznik zarządzający 13
II.1.3 Firewall 14

ROZDZIAŁ III. GWARANCJA 22

III.1.1 Usługi gwarancyjne 22

Rozdział I. Założenia początkowe oraz wymagania ogólne

I.1 Wprowadzenie

W projekcie „Informatyzacja Placówek Medycznych Województwa Świętokrzyskiego (InPlaMed WŚ), w ramach Regionalnego Programu Operacyjnego Województwa Świętokrzyskiego na lata 2014-2020 (RPOWŚ 2014-2020)", 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.

I.2 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.

I.3 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.

I.4 Opis przedmiotu 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 modernizację sieci LAN w zakresie dostawy i wdrożenia sieciowej infrastruktury sprzętowe.

POZ. OPZ	OPIS	ILOŚĆ
Rozdział II.1	**Modernizacja sieci LAN**	
AKTYWNE URZĄDZENIA SIECIOWE		
II.1.1	Przełącznik LAN	3
II.1.2	Przełącznik zarządzający	1
II.1.3	Firewall	1

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.
3. Usługi 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.
4. Wykonawca jest zobowiązany do realizacji Przedmiotu Zamówienia zgodnie z zasadami i wytycznymi Zamawiającego, niniejszymi zapisami SOPZ oraz Umowy.
5. 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 dokumentacji przetargowej 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.

6. 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.
7. 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.
8. 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 lub angielskim w formie papierowej lub elektronicznej.

I.5 Termin realizacji Przedmiotu Zamówienia

1. Termin realizacji całości Przedmiotu zamówienia wynosi **120 dni** od dnia podpisania Umowy.

I.6 Organizacja wdrożenia

I.6.1 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 Sieciowej 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.

I.6.2 Przygotowanie Dokumentacji

1. W ramach procesu prac Wykonawca opracuje dla Zamawiającego Dokumentację Przedmiotu Zamówienia (zwaną dalej Dokumentacja, Dokumentacja PZ), która składa się z nw. zakresów:
   a) Harmonogram Wdrożenia.
   b) Dokumentacja Powykonawcza.
2. 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.
3. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja Harmonogramu wdrożenia warunkuje rozpoczęcie prac Wykonawcy.
4. Harmonogram wdrożenia zostanie opracowany w oparciu o wymagania określone w niniejszym SOPZ dla części 2.

I.6.3 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.

I.6.4 Dokumentacja Powykonawcza

1. Warunkiem dokonania Odbioru Przedmiotu Umowy 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:

1) Wymogi ogólne:

1. Konfiguracja musi obejmować wszystkie urządzenia wdrożone, zainstalowane w ramach dostawy;
2. Przykładowy zestaw wymaganych danych konfiguracyjnych obejmuje:
   - sieć (adresacja IP, itp.),
   - listę zainstalowanego oprogramowania (jeżeli dotyczy),
3. Opis architektury logicznej:

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

4. Procedury lub instrukcje instalacji, reinstalacji, deinstalacji 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).
5. Procedury standardowe:
   - opis możliwości stosowania standardowych procedur poprawnej eksploatacji dla rozwiązań wspierających (sprzętowych lub aplikacyjnych).
6. Dokumentacja procesu parametryzacji:
   - wyszczególnienie wszystkich parametryzowanych elementów systemu wraz z opisem ich znaczenia i dopuszczalnych wartości oraz stosowanych wartości domyślnych.
7. Dokumenty z testów:
   - plan testów, scenariusze testowe i protokoły z testów akceptacyjnych
8. Instrukcje obsługi i instrukcje użytkowania dla wersji dostarczonego oprogramowania.

2) Wymagania szczegółowe:

1. Dokumentacja powykonawcza logicznej struktury sieci, po skonfigurowaniu klastra urządzeń UTM oraz podłączeniu hostów do sieci komputerowej powinna zawierać co najmniej:

DOKUMENTACJA POWYKONAWCZA LOGICZNEJ STRUKTURY SIECI
- Informacje ogólne
- Opis sposobu i struktury adresacji logicznej sieci
- Ogólny schemat logicznej struktury sieci

I.6.5 Odbiór Etapu/Dokumentacji/Końcowy

1. Odbiór Przedmiotu Zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy, w tym dostarczenia wymaganej zamówieniem Dokumentacji.
2. Odbiór odbędzie się zgodnie z zapisami w Umowie stanowiącej Dodatek nr 4B do SIWZ.

I.6.6 Testy

1. W ramach postępowania 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 i 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.

I.6.7 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.

I.6.8 Instruktaże stanowiskowe

1. Wykonawca zaplanuje w uzgodnieniu z Zamawiającym i przeprowadzi instruktaże stanowiskowe dla wskazanych przez Zamawiającego administratorów (min. 2 osoby) w łącznym wymiarze nie mniej niż **20** osobogodzin.
2. Podczas instruktaży stanowiskowych musi zostać przekazana niezbędna wiedza w zakresie umożliwiającym samodzielne administrowanie urządzeniami, w tym co najmniej aktualizacji firmware, konfiguracji urządzeń UTM oraz 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.

Rozdział II. Szczegółowy opis przedmiotu zamówienia

II.1 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 wyprodukowane po 1 stycznia 2019r.

II.1.1 Przełącznik LAN

Wymagane jest dostarczenie 3 szt. przełączników spełniających poniżej opisane minimalne parametry funkcjonalne:

CECHA	WYMAGANIA MINIMALNE
1. Opis techniczny	1. Minimum 48 portów 10BASE-T/100BASE-TX/1000BASE-T 2. Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP) 3. Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika) 4. Wydajność: minimum 130,9 Mp/s 5. Tablica adresów MAC o wielkości minimum 16000 pozycji 6. Bufor pakietów nie mniejszy niż 3MB 7. Pamięć stała (typu Flash): minimum 512MB 8. Pamięć operacyjna: minimum 1GB 9. Obsługa ramek Jumbo 10. Funkcja łączenia urządzeń w stosy z wykorzystaniem portów 10Gb/s i agregowanych portów 10Gb/s. Urządzenia połączone w stos widziane jako jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). 11. Dopuszcza się rozwiązanie posiadające dedykowane porty do tworzenia stosu, ale w takim przypadku wszystkie potrzebne do tego kable, moduły i licencje należy dostarczyć w ramach tego postępowania. Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 390 portów 100/1000BaseT (z obsługą i bez obsługi standardu PoE+). 12. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain)). 13. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie. 14. Routing IPv4 – minimum: statyczny (minimum 512 tras), RIP 15. Routing IPv6 – minimum: statyczny (minimum 256 tras), RIPng 16. Policy Based Routing

	17. Wsparcie dla Bidirectional Forwarding Detection (BFD) 18. Minimum 32 interfejsy IP VLAN 19. Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping 20. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol 21. Obsługa sieci IEEE 802.1Q VLAN – minimum 4094 jednoczesnych sieci VLAN 22. Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree 23. BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom 24. Wsparcie dla funcji DHCP server, DHCP Relay, DHCP client oraz DHCP Snooping (wszystkie dla IPv4 i IPv6) 25. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI 26. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia 27. Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu) 28. Obsługa standardu 802.1p – min. 8 kolejek na porcie 29. Możliwość zmiany wartości pola DSCP i wartości priorytetu 802.1p 30. Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR) lub podobny algorytm; WRR + SP 31. Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczania pasma dla ruchu określonego listą ACL z dokładnością do 64 kb/s 32. Funkcja mirroringu portów lokalnego i zdalnego: 1 to 1 Port mirroring, Many to 1 port mirroring 33. Obsługa funkcji logowania do sieci („Network Login") zgodna ze standardem IEEE 802.1x: - Możliwość przydziału stacji do wskazanej sieci wirtualnej podczas logowania IEEE 802.1x - Możliwość uwierzytelniania wielu użytkowników na jednym porcie - Przypisanie profilu QoS dla użytkownika lub grupy użytkowników 34. LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED

	35. Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC 36. TACACS+ i RADIUS Network Login 37. RADIUS Accounting 38. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS 39. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https 40. Syslog 41. Obsługa NETCONF 42. Obsługa sFlow lub NetFlow 43. Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3 44. Obsługa NTP 45. Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter. 46. Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania). 47. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji). 48. 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. onieczna 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. 49. Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego. 50. Wsparcie dla mechanizmu typu DLDP - Device Link Detection Protocol 51. Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych.

	52. Minimalny zakres pracy od -5°C do 45°C. 53. Wysokość w szafie 19" – 1U, głębokość nie większa niż 45 cm. 54. Maksymalny pobór mocy nie większy niż 100W.
2. Wyposażenie	1. Każdy przełącznik musi być wyposażony w 2 wkładki optyczne 10G LR ze złączem LC, pracujące na światłowodach jedno-modowych na odległość min. 10km 2. Każdy przełącznik musi być wyposażony w 2 kable typu DAC 10G SFP+ o długości 3 m.
3. Inne	Dopuszczalne jest zastosowanie wkładek światłowodowych SFP+ innego producenta niż przełączniki.

II.1.2 **Przełącznik zarządzający**

Wymagane jest dostarczenie 1 szt. przełącznika spełniającego poniżej opisane minimalne parametry funkcjonalne:

CECHY	WYMAGANIA MINIMALNE
1. Opis techniczny	1. Minimum 24 porty 10/100/1000BaseT 2. Minimum 4 porty Gigabitowe SFP, niezależne od wymaganych portów 10/100/1000BaseT 3. Automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT 4. Wydajność przełączania co najmniej 56 Gbps oraz przepustowość 41,6 Mpps dla pakietów 64 bajtowych 5. Obsługa 4094 tagów IEEE 802.1Q oraz minimum 512 jednoczesnych sieci VLAN 6. Funkcja łączenia w stosy (klaster) pozwalająca co najmniej na zarządzanie z poziomu jednego adresu IP minimum 9 urządzeniami. Jeżeli funkcja ta wymaga dodatkowych licencji, modułów lub kabli to Zamawiający wymaga ich dostarczenia w ramach tego postępowania. 7. Funkcja automatycznej aprowizacji i konfiguracji przełącznika przy jego pierwszym podłączeniu do sieci bez konieczności wykonywania wstępnej, ręcznej konfiguracji 8. Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az 9. Bufor pakietów nie mniejszy niż 1,5MB 10. Minimum 128MB pamięci Flash

	11. Dostęp do urządzenia przez konsolę szeregową (linia komend umożliwiająca pełne zarządzanie przełącznikiem), HTTPS, SSHv2 i SNMPv3 a. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s) b. Obsługa Secure FTP c. Obsługa 802.3ad Link Aggregation Protocol (LACP) d. Obsługa Simple Network Time Protocol (SNTP) v4 lub NTP 12. Wielkość tablicy adresów MAC: minimum 16000 13. Obsługa LLDP i LLDP-MED 14. Mechanizmy związane z zapewnieniem jakości usług w sieci: priorytetyzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek sprzętowych, rate-limiting 15. Funkcja autoryzacji użytkowników zgodna z 802.1x 16. Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+, 17. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection) 18. Obsługa list kontroli dostępu (ACL) 19. Obudowa wieżowa 1U umożliwiająca instalację w szafie 19'' o głębokości nie większej niż 45 cm. 20. Maksymalny pobór mocy nie większy niż 60W 21. Minimalny zakres pracy od 0°C do 45°C

II.1.3 Firewall

1. Wymagane jest dostarczenie 1 szt. zapory ogniowej spełniającej poniżej opisane minimalne parametry funkcjonalne.
2. W ramach realizacji zamówienia Wykonawca dostarczy, skonfiguruje, wdroży i uruchomi zaporę ogniową.
3. Ze względu na charakter działalności jaką prowadzi Zamawiający (świadczenie usług medycznych godz. 7:00 – 14:35) Wykonawca zobowiązany jest, w ramach wykonania przedmiotu umowy, do zminimalizowania przerwy w działaniu infrastruktury sieciowej ośrodka 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.
4. Założenia konfiguracyjne:

- Zapora zostanie fizycznie zainstalowana w wyznaczonym miejscu.
- Należy wykonać upgrade firmware zapory do najnowszej stabilnej wersji oprogramowania.
- Zapora zostanie dołączona do klastra/stosu przełączników macierzowych (rdzeń)

- Firewall zostanie zaadresowany zgodnie z przydzielonymi przez administratorów Zamawiającego adresami IP.
- Należy skonfigurować routing na zaporze zgodnie z zaleceniami administratorów ośrodka.
- Należy skonfigurować dostęp do urządzeń SSH oraz HTTPS, wygenerować w tym celu odpowiednie klucze RSA/DSA oraz certyfikaty.
- Należy skonfigurować niezbędne agregacje na portach przełączników macierzowych/rdzeniowych.
- Należy skonfigurować wszystkie wymagane sieci wirtualne VLAN w obrębie całej sieci oraz interfejsy VLAN.
- Sieci vlan należy przypisać do portów zgodnie z wymaganiami.
- Należy skonfigurować zabezpieczenia dostępu do zapory sieciowej.
- Należy skonfigurować użytkowników – administratorów lokalnych na urządzeniach.
- Należy skonfigurować polityki bezpieczeństwa zgodnie z tzw. Best-practices oraz zaleceniami Zamawiającego.
- Należy skonfigurować sieć DMZ.
- Należy skonfigurować funkcję NAT.
- Nalży skonfigurować usługi VPN, IPS, antywirus, web filtering itp. zgodnie z zaleceniami i tzw. best-practices.

CECHY	WYMAGANIA MINIMALNE
1. Wymagania Ogólne	1. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. 2. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. 3. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. 4. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość

	dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu. 5. System musi wspierać IPv4 oraz IPv6 w zakresie: - Firewall. - Ochrony w warstwie aplikacji. - Protokołów routingu dynamicznego.
2. Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
3. Interfejsy, Dysk, Zasilanie:	1. System realizujący funkcję Firewall musi dysponować minimum: - 20 portami Gigabit Ethernet RJ-45. - 2 gniazdami SFP 1 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.
4. Parametry wydajnościowe:	1. W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 30.000 nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 7.4 Gbps. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1 Gbps. 4. Wydajność szyfrowania IPSec VPN: nie mniej niż 4 Gbps. 5. 7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 500 Mbps.

	6. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps. 7. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 130 Mbps.
5. Funkcje Systemu Bezpieczeństwa:	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL. 12. Analiza ruchu szyfrowanego protokołem SSH.
6. Polityki, Firewall	1. System Firewall musi umożliwiać tworzenie list kontroli dostępu realizowanych bezstanowo przed funkcją FW. 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: – Translację jeden do jeden oraz jeden do wielu. – Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

7. Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: - Wsparcie dla IKE v1 oraz v2. - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode (GCM). - Obsługa protokołu Diffie-Hellman grup 19 i 20. - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. - Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
8. Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: - Routingu statycznego. - Policy Based Routingu. - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
9. Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

	3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
10. Kontrola Antywirusowa	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
11. Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
12. Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

	2. Baza Kontroli Aplikacji powinna zawierać minimum 2500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
13. Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
14. Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

15. Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
16. Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.
17. Usługi i licencje	**W ramach realizacji zamówienia powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i usług.** Powinny one obejmować: - Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego

	Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.

Rozdział III. Gwarancja

1. Wykonawca w ramach realizacji Przedmiotu Zamówienia udzieli Zamawiającemu gwarancji jakości (dalej zwanej „gwarancją") na niniejszy przedmiot zamówienia:

   1) **modernizacja sieci LAN** w zakresie dostawy i wdrożenia Infrastruktury aktywnej sieci

POZ. OPZ	OPIS	OKRES GWARANCJI (MINIMALNY)
AKTYWNE URZĄDZENIA SIECIOWE		
II.1.1	Przełącznik LAN	60 miesięcy gwarancji producenta. obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory)
II.1.2	Switch zarządzający	
II.1.3	Firewall	

2. Bieg terminów gwarancji określonych w ust. 1 będą rozpoczynać się z dniem podpisania Protokołu Odbioru Końcowego bez uwag przez Zamawiającego.
3. W ramach gwarancji należy zapewnić również dostęp do aktualizacji oprogramowania oraz wsparcia technicznego w dni robocze pomiędzy godz. 8.00 a 16.00.
4. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis.

III.1.1 Usługi gwarancyjne

1. W okresie gwarancji Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu rozumianych jako Awaria lub Usterka zgodnie z definicjami jak poniżej:
   1) **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.
   2) **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.

2. Przyjęcie zgłoszenia przez Wykonawcę, odbywać się będzie w okresie dostępności Wykonawcy wskazanym 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:
   1) System Zgłoszeń dostarczy Wykonawca (będzie on utrzymywany i administrowany przez Wykonawcę), wpis zgłoszenia do SZ będzie dokonywał Zamawiający.
   2) Za skuteczne przyjęcie zgłoszenia 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.
3. Gwarancja musi zapewniać wymianę uszkodzonego sprzętu, kabli i elementów oraz zapewniać dostęp do aktualizacji oprogramowania, bez wiedzy i wsparcia technicznego producenta.
4. W ramach gwarancji Wykonawca będzie świadczył następujące usługi:
   1) 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

<table>
<tr><th>KWALIFIKACJA ZGŁOSZENIA WADY</th><th>OKRES DOSTĘPNOŚCI WYKONAWCY</th><th>ROZWIĄZANIE ZASTĘPCZE</th><th>CZAS REAKCJI WYKONAWCY</th><th>CZAS NAPRAWY</th></tr>
<tr><td>AWARIA</td><td rowspan="2">24/7/365</td><td>niezwłocznie, nie później niż 24 godzin od czasu przyjęcia zgłoszenia</td><td>niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia</td><td>niezwłocznie, nie później niż 10 dni od czasu przyjęcia zgłoszenia</td></tr>
<tr><td>USTERKA</td><td>nie dotyczy</td><td>niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia</td><td>niezwłocznie nie później niż 30 dni od dnia przyjęcia zgłoszenia</td></tr>
</table>

   2) dopuszcza się zmianę kwalifikacji zgłoszenia Wady, po uprzedniej zgodzie Zamawiającego. Do czasu potwierdzenia zmiany kwalifikacji, uznaje się za obowiązującą kwalifikację pierwotną,

3) czasy naprawy mogą być inne niż wskazane w powyższej tabeli, jeżeli Zamawiający zaakceptuje zmianę kwalifikacji zgłoszenia, o której mowa w punkcie 2),

4) w przypadku braku możliwości usunięcia Wady lub przedstawienia rozwiązania zastępczego zdalnie, Wykonawca zobowiązany jest do świadczenia gwarancji bezpośrednio w lokalizacji Zamawiającego,

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 7.00 do 14.35 w każdym Dniu Roboczym.

W innych przypadkach należy rozumieć jako dzień kalendarzowy.