Program Funkcjonalno-Użytkowy

do postepowania o nazwie:

„Budowa serwerowni oraz systemu zabezpieczeń systemów informatycznych w Szpitalu Wojewódzkim im. Świętego Łukasza w Tarnowie”

Zamawiający i adres obiektu:	Szpital Wojewódzki im. Św. Łukasza Samodzielny Publiczny Zakład Opieki Zdrowotnej w Tarnowie ul. Lwowska 178A 33-100 Tarnów

Spis treści

Spis rysunków

Kody CPV

1. 32422000-7 Elementy składowe sieci
2. 453 00000-0 Roboty w zakresie instalacji budowlanych.
3. 453 10000-3 Roboty instalacyjne elektryczne.
4. 71024000-2 Usługi architektoniczne, inżynieryjne i planowania

Preambuła – skrócony opis przedmiotu zamówienia

Przedmiotem niniejszego zamówienia jest w szczególności:

- Wykonanie i dostarczenie dokumentacji projektowej
- Budowa nowej serwerowni
- Dostawa, montaż i uruchomienie systemu klimatycznego
- Dostawa, montaż i uruchomienie systemu gaszenia
- Uruchomienie systemu nadzoru środowiskowego serwerowni
- Dostawa i montaż okablowania strukturalnego
- Dostawa, montaż i uruchomienie punktów dostępowych sieci WiFi
- Dostawa, montaż i uruchomienie nowych zasobów sieciowych
- Dostawa, montaż i uruchomienie systemu bezpieczeństwa informatycznego
- Przeniesienie sprzętu ze starej serwerowni do nowej.
- Testy i uruchomienie
- Szkolenia
- Odbiór końcowy oraz rozpoczęcie świadczenia usług serwisowych.

Preambuła – cel projektu

Celem projektu jest uruchomienie nowej serwerowni dla systemów infrastruktury IT Szpitala, w sposób taki aby zabezpieczyć działanie obecnej serwerowni, a w przyszłości przenieść obecnie funkcjonującą serwerownię do serwerowni planowanej do wykonania w nowym budynku. Serwerownia objęta niniejszym projektem wraz z planowaną w nowym budynku serwerownią stanowić będzie docelowe rozwiązanie w Szpitalu. Celem projektu jest też wdrożenie zaawansowanych systemów bezpieczeństwa, umożliwiających ochronę danych osobowych i danych medycznych istniejących w szpitalu oraz ochronę bazy danych.

Do wykonawcy będzie należało przede wszystkim wybudowanie nowej serwerowni od nowa w pomieszczeniach wskazanych przez Szpital, wraz z instalacjami niezbędnymi do jej normalnego funkcjonowania, wykonanie niezbędnego połączenia pomiędzy serwerownią nową i starą, wdrożenie systemów zabezpieczeń IT oraz przeniesienie serwerów i macierzy do nowej serwerowni w sposób zapewniający dualizm rozwiązań. Do zadań wykonawcy będzie również należało uruchomienie nowej struktury sieciowej w szpitalu (na poziomie połączeń pomiędzy serwerownią i PD) oraz zainstalowanie infrastruktury niezbędnej do rozwoju systemu WiFi.

Słowniczek

Pojęcie/ Skrót	Opis
6A	Kategoria okablowania strukturalnego miedzianego zgodnego z normami TIA ANSI/TIA//EIA-568-B.2.10 Commercial Building Telecommunications Standard Part 2: Addendum 10: Transmission Performance Specification for 4 Pair 100 Ohm Augmented Category 6 cabling draft, zapewniająca prawidłowe połączenia w sieciach 10GE (zgodnie z ISO kat EA)
Administrator	Administrator Systemów Informatycznych - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego
Analiza Przedwdrożeniowa	Należy przez to rozumieć etap Umowy obejmujący uzgodnienia i wykonanie przez Wykonawcę DAP wraz z Harmonogramem wdrożenia.
Analiza wymagań	Należy przez to rozumieć zakres czynności do wykonania przez Wykonawcę w Analizie Przedwdrożeniowej polegający na szczegółowym zrozumieniu, doprecyzowaniu i dookreśleniu wymagań Zamawiających.
AP	Access Point – punkt dostępu do bezprzewodowej sieci komputerowej
Awaria	Kategoria Wady w Infrastrukturze sprzętowej pasywnej lub Infrastrukturze sieciowej oznaczająca brak działania lub niepoprawne działanie PZ u Zamawiającego, uniemożliwiające jego użytkowanie. Sytuacja, w której infrastruktura w ogóle nie funkcjonuje lub nie jest możliwe realizowanie istotnych funkcjonalności Komponentów/Produktów zamówienia
AWG	American Wire Gauge – skala grubości skrętki LAN (18 do 24 AWG)
CA	Certificate Authority – centrum certyfikacji jako zespół środków organizacyjno-technicznych, wystawiające certyfikaty cyfrowe dla potrzeb autoryzacji uprawnień dostępu do systemów informatycznych
CCTV	System Telewizji Dozorowej
CE	Conformité Européenne – oznaczenie wyrobu potwierdzające zgodność z zasadniczymi wymaganiami bezpieczeństwa obowiązującymi w Unii Europejskiej; umieszczone na wyrobie jest deklaracją producenta, że oznakowany wyrób spełnia wymagania dyrektyw tzw. "Nowego Podejścia" Unii Europejskiej (UE).
CIFS	Common Internet File System – protokół służący udostępnianiu zasobów komputerowych
CLOUD	Chmura – odmiejscowiona struktura obliczeniowa lub niezawodnościowa

Pojęcie/ Skrót	Opis
	umieszczona w różnych ośrodkach przetwarzania danych
Czas naprawy	Należy przez to rozumieć czas, jaki może upłynąć pomiędzy pierwszym zgłoszeniem Wady, a Usunięciem Wady.
Czas Reakcji Wykonawcy	Należy przez to rozumieć maksymalny czas jaki może upłynąć pomiędzy pierwszym zgłoszeniem Wady a podjęciem działań przez Wykonawcę. Przez działania Wykonawcy rozumie się co najmniej dla wykonanych Robót budowlanych: podjęcie czynności technicznych w lokalizacji Zamawiającego zmierzających do usunięcia Wady
DC	Direct Current – prąd stały
DHCP	Dynamic Host Configuration Protocol - protokół dynamicznego konfigurowania hostów
DMZ	Demilitarized zone, strefa zdemilitaryzowana bądź ograniczonego zaufania – jest to wydzielany na zaporze sieciowej (ang. Firewall/UTM) obszar sieci komputerowej nienależący ani do sieci wewnętrznej (tj. tej chronionej przez zaporę), ani do sieci zewnętrznej (tej przed zaporą; na ogół jest to Internet).
Dni robocze	Dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy, wskazanych w ustawie z dnia 18 stycznia 1951 r o dniach wolnych od pracy (tj Dz. U. z 2020 r. poz. 1920)
DNS	Domain Name System - system nazw domenowych
Dokumentacja Przedmiotu Zamówienia (Dokumentacja, Dokumentacja PZ)	Wszelka dokumentacja dostarczona przez Wykonawcę, związana z PZ i powstała w wyniku realizacji Umowy zawartej pomiędzy Zamawiającym, a Wykonawcą. Dokumentacja zawiera: Dokumentację Analizy Przedwdrożeniowej (DAP), Dokumentację Projektową (DPR), (projekty wykonawcze branżowe, projekty technologiczne, projekty techniczne, pozostałe dokumenty projektowe), Dokumentację Powykonawczą (DPO), Dokumentację użytkową (DU)
Dokumentacja Analizy Przedwdrożeniowej (DAP)	Dokumentacja opracowana przez Wykonawcę wraz z późniejszymi zmianami (jednakowa dla poszczególnych części jednego Wykonawcy w zakresie wspólnym), na podstawie której będzie realizowany organizacyjnie i technicznie PZ, która będzie podlegała uzgodnieniu i akceptacji Zamawiającego zawierająca w szczególności: Harmonogram wdrożenia zawierający elementarne zadania do wykonania

Pojęcie/ Skrót	Opis
	podczas realizacji PZ: Terminy prac Wykonawcy na wykonanie poszczególnych Komponentów, Etapów, Przedmiotu Zamówienia Terminy iteracji testów oraz terminy odbiorów, o których mowa w Procedurze testowania" oraz „Procedurze odbiorowej". Podział PZ na Produkty, a następnie pogrupowanie ich w Komponenty Zasady organizacji w realizacji PZ Plan komunikacji Zamawiającego z Wykonawcą Analizę wymagań Przedmiotu Zamówienia zawierającą opis sposobu realizacji każdego wymagania, sposób testowania i odbioru, Karty katalogowe potwierdzające spełnienie wymagań, Dokumentacje i plan dostaw, Opis modernizacji i budowy Infrastruktury sprzętowej, Dokumentacje i plany testów, o którym mowa w „Procedurze testowania", Dokumentacje i plany odbiorów, o którym mowa w „Procedurze odbiorowej", Listę Komponentów, które będę podlegały osobnym odbiorom. Szczegółowe uzgodnienia Stron Umowy dotyczące zakresu i sposobu integracji dostarczanych rozwiązań z Istniejącą infrastrukturą, Zakres prac realizowanych przez podwykonawców, Szczegółowy zakres i zawartość Dokumentacji urządzeń aktywnych, Dokumentacji projektowej, Dokumentacji powykonawczej i Dokumentacji użytkowej w podziale na Zamawiających. Opis wszystkich elementów oprogramowania wdrażanego w trakcie projektu i sposobie ich instalacji w infrastrukturze.
Dokumentacja Powykonawcza (DPO)	Należy przez to rozumieć dokumenty zawierające dokładną konfigurację Komponentów na moment podpisania Protokołu odbioru końcowego, w tym co najmniej: Dokumentacja budowlana (o ile jest wymagana) powykonawcza (zgodna z przepisami, w szczególności obejmująca projekt, protokoły odbiorów częściowych i końcowych, rysunki i opisy służące realizacji projektu, operaty geodezyjne, książki obmiaru, geodezyjne pomiary powykonawcze, projekty sieci

Pojęcie/ Skrót	Opis
	radiowej itp.) Schemat architektury Infrastruktury sprzętowej wraz z połączeniami poszczególnych ich elementów z dokładnością do rodzajów technologii Wykaz elementów Infrastruktury sprzętowej obejmujący ich kompletne specyfikacje m.in. nazwę producenta, typ, model, miejsce instalacji, etc. Wykaz Oprogramowania niezbędnego do działania Komponentów o ile to Oprogramowanie jest niezbędne; Instrukcje instalacji, obsługi, zarządzania i konfiguracji wszystkich elementów Infrastruktury sprzętowej niezbędnych do działania dostarczanego rozwiązania; Wykaz zalecanych parametrów Infrastruktury niezbędnych do prawidłowego funkcjonowania wdrożonych Komponentów; Opis konfiguracji adresowany do Administratora, pozwalający na samodzielne administrowanie dostarczonym w ramach zamówienia rozwiązaniem przez Zamawiających po dokonaniu Odbioru końcowego; Szczegółowe informacje na temat zmian poczynionych w konfiguracji, parametryzacji i ustawieniach istniejącej sieci LAN u danego Zamawiającego Procedury serwisowe wszystkich elementów dostarczonej Infrastruktury Inne dokumenty wytworzone w trakcie realizacji PZ dotyczące rozwiązań technicznych i projektowych. Opis wszystkich elementów oprogramowania wdrażanego w trakcie projektu i sposobie ich instalacji w infrastrukturze.
Dokumentacja Projektowa (DPR)	Dokumentacja (w tym projekty wykonawcze branżowe w szczególności konstrukcyjne, telekomunikacyjne, instalacyjne elektryczne, instalacyjne sanitarne) opracowana przez Wykonawcę wraz z późniejszymi zmianami, na podstawie której będzie realizowany PZ i która będzie podlegała uzgodnieniom i akceptacji Zamawiających oraz Inspektora Nadzoru IK. Rozpoczęcie realizacji instalacji, konfiguracji i wdrożenia Infrastruktury będzie każdorazowo możliwe po uzgodnieniu, a następnie odbiorze Dokumentacji projektowej przez Zamawiających. Minimalny zakres DPR: Koncepcja: Część opisowa

Pojęcie/ Skrót	Opis
	Schematy blokowe projektowanej instalacji zasilającej Schematy blokowe projektowanej instalacji światłowodowej Projekt budowlany wraz z pozwoleniem na budowę o ile jest wymagany Rzuty budynków z rozmieszczeniem projektowanych urządzeń Przebieg projektowanej zewnętrznej kanalizacji teletechnicznej sporządzony na aktualnej mapie do celów projektowych Projekt wykonawczy: Część opisowa zawierająca szczegółowe rozwiązana projektowe wraz z załączonymi kartami katalogowymi projektowanych urządzeń Rzuty budynków z rozmieszczeniem projektowanych rozdzielnic, UPS-ów, punktów PEL i PL oraz przebiegiem tras kablowych. Przebieg projektowanej zewnętrznej kanalizacji teletechnicznej Schematy jednokreskowe projektowanych rozdzielnic elektrycznych Schematy jednokreskowe połączeń światłowodowych W przypadku projektów z serwerowniami rzuty z domiarem urządzeń w serwerowni Specyfikacje techniczne Wykonania i odbioru robót Harmonogramu rzeczowo-finansowego
Dokumentacja użytkowa (DU)	Należy przez to rozumieć dokumenty będące instrukcjami obsługi, które w przystępny sposób pokazują jak Użytkownik wewnętrzny ma się posługiwać Infrastrukturą, aby całkowicie samodzielnie administrować dostarczanym rozwiązaniem obejmujące w minimalnym zakresie. instrukcje konfiguracji i administracji, instrukcje postępowania w przypadkach szczególnych oraz awarii, instrukcje konserwacji.
Dostawy	Należy przez to rozumieć dostarczenie do siedziby Zamawiającego lub miejsca

Pojęcie/ Skrót	Opis
	przez niego wskazanego elementów PZ, które może obejmować dodatkowo rozmieszczenie lub instalację;
DR	Disaster Recovery – odtwarzanie awaryjne/zapasowe centrum danych
EMF	ElectroMagnetic Field – Pole Elektromagnetyczne
ESD	Elektroniczny System Dostępu
FC	Fibre Channel - standard magistrali szeregowej definiujący wielowarstwową architekturę, która służy do przesyłania danych przez sieć.
Harmonogram wdrożenia	Szczegółowy harmonogram wdrożenia, opracowany przez Wykonawcę na podstawie SIWZ podczas Analizy Przedwdrożeniowej.
IBWR	Instrukcja Bezpiecznego Wykonywania Robót zgodna z § 2 Rozporządzenia Ministra Infrastruktury z dnia 6 lutego 2003 r. w sprawie bezpieczeństwa i higieny pracy podczas wykonywania robót budowlanych (Dz.U. nr 23, poz. 401)
IDC	Insulated Displacement Connector – złącze izolowane
IDF / PD	Indirect Distribution Frame – inaczej Punkt Dystrybucyjny (PD). Lokalny punkt dystrybucyjny obsługujący najczęściej dany obszar roboczy lub piętro.
Infrastruktura sieciowa (aktywna)	Urządzenia sieci przewodowej i bezprzewodowej oraz wszelkie urządzenia dodatkowe np. serwery, służące do obsługi infrastruktury sieciowej i urządzeń końcowych.
Infrastruktura sieciowa	Urządzenia i pasywne elementy sieci komputerowych LAN dostarczane przez Wykonawcę wchodzące w skład wdrażanego u Zamawiających rozwiązania będące częścią Robót budowalnych obejmujące w szczególności: część pasywną sieci komputerowych LAN: kable, gniazda sygnałowe i elektryczne, panele, organizery, trasy kablowe, etc., wyposażenie pomieszczeń technicznych takich jak szafy i przełącznice pozostałe instalacje elektryczne i systemy budynkowe
Infrastruktura sprzętowa pasywna	Rozumiane jako urządzenia: UPS, Klimatyzator, CCTV, SSWiN, KD, VESDA, SUG, System monitorowania infrastruktury i warunków klimatycznych w serwerowni – wskazane rodzajowo w PFU.
IPS	Intrusion Prevention System – systemy wykrywania i zapobiegania włamaniom
Komitet sterujący	Należy przez to rozumieć zespół osób składający się z przedstawicieli Zamawiającego, których zadaniem jest podejmowanie kluczowych decyzji oraz

Pojęcie/ Skrót	Opis
	nadzorowanie realizacji PZ.
Komponent	Komponent to integralna część dostawy i wdrożenia PZ. Komponent powinien się składać przynajmniej z jednego Produktu lub wielu Produktów powiązanych ze sobą merytorycznie. Podstawowy podział Komponentów oczekiwany przez Zamawiających: Sieci okablowania strukturalnego LAN Infrastruktura zasilania gwarantowanego Infrastruktura klimatyzacji i wentylacji Systemy zabezpieczeń.
KD	Kontrola Dostępu
LAN	Local Area Network – lokalna sieć komputerowa
LC	Little Connector – standard rozłączalnego połączenia dwóch światłowodów charakteryzujące się małymi wymiarami i blokadą zatrzaskową
LDAP	Lightweight Directory Access Protocol - protokół przeznaczony do korzystania z usług katalogowych wykorzystywany głównie dla baz danych w szczególności zawierających dane identyfikacyjne.
LSFRZH	Standard materiału z którego wykonany jest kabel światłowodowy - powłoka z materiału niepalnego, powłoka bezhalogenowa
LSZH	Standard materiału z którego wykonany jest kabel światłowodowy - tworzywo bezhalogenowe, nierozprzestrzeniające płomienia o ograniczonym wydzielaniu dymu oraz gazów toksycznych i korozyjnych
MAN	Metropolitan Area Network –miejska sieć komputerowa
MDF	Main Distribution Frame - Punkt Dystrybucyjny sieci LAN
MM	MultiMode – Światłowód Wielomodowy
MPŚ	Monitoring Warunków Środowiskowych
MVPN/MPLS VPN	Wirtualna Sieć Prywatna w sieci MPLS
NAS	Network Attached Storage - technologia umożliwiająca podłączenie zasobów pamięci dyskowych bezpośrednio do sieci komputerowej
NEXT	Near End Cross Talk - przesłuch sygnału na bliskim końcu kabla LAN

Pojęcie/ Skrót	Opis
NFS	Network File System – oparty na UDP lub TCP protokół zdalnego udostępniania systemu plików
Odbiór częściowy	Należy przez to rozumieć odbiór robót ulegających zakryciu
Odbiór etapu	Należy przez to rozumieć odbiór etapu Umowy, zgodny z SIWZ i Dokumentacją Analizy przedwdrożeniowej.
Odbiór końcowy	Należy przez to rozumieć odbiór końcowy PZ zgodny z wymogami SIWZ w tym z postanowieniami Dokumentacji Analizy Przedwdrożeniowej.
Okres dostępności Wykonawcy	Należy przez to rozumieć przedział czasu w jakim Wykonawca jest gotowy do przyjęcia zgłoszenia Wad
OM	Optical Multimode – kategoria wydajności transmisyjnej dotycząca światłowodów wielomodowych
OS	Optical Singlemod – kategoria wydajności transmisyjnej dotycząca światłowodów jednomodowych
PD	Punkt Dystrybucyjny będący szafą PD, zlokalizowany w pomieszczeniu przeznaczonym pod punkt dystrybucyjny lub w innych pomieszczeniach jako szafa wisząca.
PEL i PL	Punkt Elektryczno-Logiczny sieci LAN składający się z jednego gniazdka zasilania i jednego gniazdka RJ45 i Punk Logiczny sieci LAN składający się z jednego gniazdka RJ45
PFU	Program Funkcjonalno – Użytkowy
PiMF	Pairs in Metal Foil - skrętka z każdą parą foliowaną dodatkowo w ekranie z siatki
PKI (CA)	Public Key Infrastructure (Certification Authority) - Infrastruktura klucza publicznego
PoE	Power over Ethernet - technologia przesyłu energii elektrycznej za pomocą skrętki do urządzeń peryferyjnych będących elementami sieci Ethernet
Produkt	Elementarny efekt działań/prac/dostaw objętych całym zakresem Przedmiotu Zamówienia wykonywanych przez Wykonawcę podczas realizacji Umowy w poszczególnych etapach
Protokół odbioru etapu	Protokół, który po podpisaniu bez zastrzeżeń przez Zamawiającego oraz IN stanowi potwierdzenie wykonania prac przewidzianych w ramach etapów określonych w SIWZ i uszczegółowionych w Dokumentacji Analizy przedwdrożeniowej.

Pojęcie/ Skrót	Opis
Protokół odbioru końcowego	Protokół, który po podpisaniu bez zastrzeżeń przez Zamawiającego oraz IK stanowi potwierdzenie wykonania i odbioru przedmiotu zamówienia.
Protokół rozbieżności	Protokół (zaakceptowany przez IN), w którym Zamawiający wskazuje zastrzeżenia co do zakresu i jakości wykonanych prac, które uniemożliwiają dokonanie odbioru wykonanych prac.
PSNEXT	Power Sum NEXT - suma mocy przesłuchów w bliskim końcu kabla LAN
PSELFEXT	Power Sum ELFEXT - suma mocy poziomu równoważnego dalekiego końca przesłuchu kabla LAN
PVC	Polyvinyl Chloride – Polichlorek Winylu – polimer syntetyczny
RD	Rozdzielnia Dystrybucyjna
RG	Rozdzielnia Główna – główny element sieci elektrycznej zawierający urządzenia i podzespoły służące do łączenia, przerywania oraz rozdziału obwodów elektrycznych
RGNN	Rozdzielnica Główna Niskiego Napięcia
RHDPE	Rura czarna z wewnętrzną ścianką rowkowaną wzdłużnie oraz z warstwą poślizgową
SAD	System Archiwizacji Danych
SAS	Serial Attached SCSI - interfejs komunikacyjny, będący następcą SCSI
Serwis	Zespół czynności niezbędnych do zachowania gwarancji producenta (niezbędne przeglądy konserwacje i in.), wykonywany na zasadach wymaganych przez producenta (bez uwzględnienia materiałów eksploatacyjnych).
S/FTP	Skrętka z każdą parą foliowaną dodatkowo w ekranie z siatki.
Site Survey	Proces planowania i budowania nowej sieci bezprzewodowej. Polega na analizie terenu i jego możliwości pod kątem instalacji sieci bezprzewodowej
SKD	System Kontroli Dostępu
SIWZ	Specyfikacja Istotnych Warunków Zamówienia
SM	SingleMode – Światłowód Jednomodowy
SSID	Service Set Identifier - identyfikator sieci WLAN
SSO	Single sign-on – system pojedynczego logowania

Pojęcie/ Skrót	Opis
SSWiN	System Sygnalizacji Włamania i Napadu
SUG	Stałe Urządzenie Gaśnicze
SWiN	Sygnalizacja Włamania i Napadu
SZR lub AZR	Samoczynne (Automatyczne) Załączanie Rezerwy
UA	Urządzenia aktywne LAN, np. przełączniki sieciowe, routery, sprzętowe kontrolery sieciowe, punkty dostępowe AP, wkładki optyczne, itp.
UK	Usługa Katalogowa
Umowa	Umowa w sprawie zamówienia publicznego pomiędzy Zamawiającym i Wykonawcą na wykonanie Przedmiotu Zamówienia.
Usterka	Należy przez to rozumieć kategorię Wady w Infrastrukturze sprzętowej pasywnej lub Infrastrukturze sieciowej oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz SIWZ, nie wpływającą istotnie na pracę dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi Zamawiającego.
Usunięcie Wady	Należy przez to rozumieć wykonanie prac w Przedmiocie Zamówienia przez Wykonawcę, w wyniku których nastąpi przywrócenie do stanu sprzed wystąpienia Wady wraz z usunięciem jej skutków.
UPS	Uninterruptible Power Supply – zasilacz awaryjny
Urządzenia Aktywne	Wszystkie urządzenia i sprzęt infrastruktury aktywnej, np. routery, przełączniki, AP, kontrolery, wkładki sfp, serwery, macierze i inne,
Urządzenia pasywne	Wszystkie urządzenia wyposażenia serwerowni oraz kable, np. przewody, gniazdka, koryta, kable, moduły połączeniowe, krosownice, szafy RACK, urządzenia SUG, SSWiN, WLZ, KD (SKD) itp.
UTM	Unified Threat Management - wielofunkcyjne zapory sieciowe zintegrowane w postaci jednego urządzenia i/lub oprogramowania
Użytkownik wewnętrzny	Należy przez to rozumieć pracownika lub osobę upoważnioną przez Zamawiającego, posiadającą uprawnienia do korzystania z Oprogramowania i/lub Sprzętu
VESDA	Very Early Smoke Detection Apparatus – System Wczesnej Detekcji Dymu
VFI	Voltage Frequency Independent - napięcie wyjściowe UPS nie zależy od wartości napięcia i częstotliwości napięcia zasilającego UPS

Pojęcie/ Skrót	Opis
VLAN	Virtual Local Area Network - sieć komputerowa wydzielona logicznie w ramach innej, większej sieci fizycznej
VPN	Virtual Private Network - Wirtualna Sieć Prywatna
Wada	Należy przez to rozumieć Wadę Infrastruktury sprzętowej pasywnej, Wadę Infrastruktury sieciowej, Wadę budowlaną
Wada Infrastruktury sprzętowej pasywnej	Należy przez to rozumieć Awarię lub Usterkę w Infrastrukturze sprzętowej pasywnej
Wada Infrastruktury sieciowej	Należy przez to rozumieć Awarię lub Usterkę w Infrastrukturze sieciowej
WAN	Wide Area Network – Komputerowa Sieć rozległa
Wdrożenie	Należy przez to rozumieć, wszelkie prace prowadzone przez Wykonawcę
Wiegand	Standard kontroli dostępu realizowany transmisją 2 przewodową
WLAN lub WiFi	Wireless Local Area Network – bezprzewodowa lokalna sieć komputerowa stanowiąca podzbiór LAN
WLZ	Wewnętrzna Linia Zasilająca
Wykonawca	Podmiot wyłoniony w trakcie postępowania przetargowego realizujący PZ.
Zamawiający	Szpital Wojewódzki im. św. Łukasza w Tarnowie
Zespół Zarządzania	Wyznaczone osoby po stronie Zamawiającego, IN i Wykonawcy, których zadaniem jest podejmowanie decyzji operacyjnych dotyczących realizacji Umowy
Zgłoszenie Wady	Zdarzenie, w wyniku którego nastąpiło powiadomienie Wykonawcy o zaistniałej Wadzie.

1. Opis stanu aktualnego – tabele inwentaryzacji

1.1.Urządzenia sieciowe – stan obecny

1		Dostawca	Adres
		Tarnowski Ośrodek Informacyjny	ul. Nowy Świat 3; 33-100 Tarnów
2	Przepustowość sieci wewnętrznej w lecznictwie (część biała) [Mbps]		1000
3	Przepustowość sieci wewnętrznej w administracji placówki (część szara) [Mbps]		1000
4	Czy istnieje główny węzeł sieci lokalnej? (TAK / NIE)		TAK
5	Czy główny węzeł sieci lokalnej zlokalizowany jest w serwerowni placówki? (TAK / NIE)		TAK
6	Czy istnieją węzły dystrybucyjne sieci loklanej? (TAK / NIE) oraz ich ilość.	TAK / NIE	Ilość
		TAK	43
7	Opis głównego węzła sieci lokalnej. (D2_Informatycy)		
		Ogólna liczba portów LAN	384
		Liczba zajętych portów LAN	214
		Liczba wolnych portów LAN	170
		Ogólna liczba przełączników poziomu dostępowego	5

		Ogólna liczba przełączników poziomu szkieletowego	4
		Ogólna liczba routerów	3
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	1
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	1
8	Opis węzła (-ów) dystrybucyjnego (-ych) sieci lokalanej. (A2_Ortopedia)		
		Ogólna liczba portów LAN	124
		Liczba zajętych portów LAN	104
		Liczba wolnych portów LAN	20
		Ogólna liczba przełączników poziomu dostępowego	2
		Ogólna liczba przełączników poziomu szkieletowego	2
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#2 B1_RTG		
		Ogólna liczba portów LAN	132
		Liczba zajętych portów LAN	82
		Liczba wolnych portów LAN	50
		Ogólna liczba przełączników poziomu dostępowego	4
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	1
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#3 B0_Analityka		
		Ogólna liczba portów LAN	72

		Liczba zajętych portów LAN	60
		Liczba wolnych portów LAN	12
		Ogólna liczba przełączników poziomu dostępowego	3
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#4 B1_Onkologia		
		Ogólna liczba portów LAN	48
		Liczba zajętych portów LAN	36
		Liczba wolnych portów LAN	12
		Ogólna liczba przełączników poziomu dostępowego	2
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#5 B2_USG		
		Ogólna liczba portów LAN	24
		Liczba zajętych portów LAN	15
		Liczba wolnych portów LAN	9
		Ogólna liczba przełączników poziomu dostępowego	1
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#6 D0_Poradnie		
		Ogólna liczba portów LAN	96
		Liczba zajętych portów LAN	90
		Liczba wolnych portów LAN	6

		Ogólna liczba przełączników poziomu dostępowego	2
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#7 D1_ChemDz		
		Ogólna liczba portów LAN	48
		Liczba zajętych portów LAN	46
		Liczba wolnych portów LAN	2
		Ogólna liczba przełączników poziomu dostępowego	1
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#8 E2_BlokOp		
		Ogólna liczba portów LAN	12
		Liczba zajętych portów LAN	12
		Liczba wolnych portów LAN	0
		Ogólna liczba przełączników poziomu dostępowego	1
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#9 E1_Anestezjologia		
		Ogólna liczba portów LAN	24
		Liczba zajętych portów LAN	4
		Liczba wolnych portów LAN	20
		Ogólna liczba przełączników poziomu dostępowego	1

		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#10 A0_Angiokardiografia		
		Ogólna liczba portów LAN	72
		Liczba zajętych portów LAN	36
		Liczba wolnych portów LAN	36
		Ogólna liczba przełączników poziomu dostępowego	3
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#11 A0_Endoskopia		
		Ogólna liczba portów LAN	
		Liczba zajętych portów LAN	
		Liczba wolnych portów LAN	
		Ogólna liczba przełączników poziomu dostępowego	
		Ogólna liczba przełączników poziomu szkieletowego	
		Ogólna liczba routerów	
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	
8	#12 A1_Rehabilitacja		
		Ogólna liczba portów LAN	24
		Liczba zajętych portów LAN	11
		Liczba wolnych portów LAN	13
		Ogólna liczba przełączników poziomu dostępowego	1
		Ogólna liczba przełączników poziomu szkieletowego	

		Ogólna liczba routerów	
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	
8	#13 A3_ChirOg		
		Ogólna liczba portów LAN	48
		Liczba zajętych portów LAN	21
		Liczba wolnych portów LAN	27
		Ogólna liczba przełaczników poziomu dostępowego	1
		Ogólna liczba przełaczników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#14 A4_Wewn2		
		Ogólna liczba portów LAN	24
		Liczba zajętych portów LAN	23
		Liczba wolnych portów LAN	1
		Ogólna liczba przełaczników poziomu dostępowego	1
		Ogólna liczba przełaczników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#15 A5_Kardiologia		
		Ogólna liczba portów LAN	48
		Liczba zajętych portów LAN	38
		Liczba wolnych portów LAN	10
		Ogólna liczba przełaczników poziomu dostępowego	1
		Ogólna liczba przełaczników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu	0

		firewall/UTM	
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#16 A5_Informatycy		
		Ogólna liczba portów LAN	48
		Liczba zajętych portów LAN	40
		Liczba wolnych portów LAN	8
		Ogólna liczba przełaczników poziomu dostępowego	2
		Ogólna liczba przełaczników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#17 A6_Urologia		
		Ogólna liczba portów LAN	48
		Liczba zajętych portów LAN	36
		Liczba wolnych portów LAN	12
		Ogólna liczba przełaczników poziomu dostępowego	1
		Ogólna liczba przełaczników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#18 A7_Okulistyka		
		Ogólna liczba portów LAN	24
		Liczba zajętych portów LAN	15
		Liczba wolnych portów LAN	9
		Ogólna liczba przełaczników poziomu dostępowego	1
		Ogólna liczba przełaczników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu	0

		IDS/IPS	
8	#19 C1_SOR		
		Ogólna liczba portów LAN	24
		Liczba zajętych portów LAN	23
		Liczba wolnych portów LAN	1
		Ogólna liczba przełączników poziomu dostępowego	1
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#20 C1_SOR_URAZ		
		Ogólna liczba portów LAN	48
		Liczba zajętych portów LAN	44
		Liczba wolnych portów LAN	4
		Ogólna liczba przełączników poziomu dostępowego	2
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#21 C2_BlokPor		
		Ogólna liczba portów LAN	24
		Liczba zajętych portów LAN	10
		Liczba wolnych portów LAN	14
		Ogólna liczba przełączników poziomu dostępowego	1
		Ogólna liczba przełączników poziomu szkieletowego	
		Ogólna liczba routerów	
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	
8	#22 H piwnica_Magazyn		

		Ogólna liczba portów LAN	48
		Liczba zajętych portów LAN	16
		Liczba wolnych portów LAN	32
		Ogólna liczba przełączników poziomu dostępowego	2
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#23 H0_Neurologia		
		Ogólna liczba portów LAN	24
		Liczba zajętych portów LAN	13
		Liczba wolnych portów LAN	11
		Ogólna liczba przełączników poziomu dostępowego	1
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#23 H1_Pediatria		
		Ogólna liczba portów LAN	48
		Liczba zajętych portów LAN	31
		Liczba wolnych portów LAN	17
		Ogólna liczba przełączników poziomu dostępowego	2
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#24 H2_Otolaryngologia		
		Ogólna liczba portów LAN	24
		Liczba zajętych portów LAN	12

		Liczba wolnych portów LAN	12
		Ogólna liczba przełączników poziomu dostępowego	1
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#25 H3_ChirDz		
		Ogólna liczba portów LAN	34
		Liczba zajętych portów LAN	23
		Liczba wolnych portów LAN	11
		Ogólna liczba przełączników poziomu dostępowego	2
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#26_H2_Noworodki		
		Ogólna liczba portów LAN	24
		Liczba zajętych portów LAN	14
		Liczba wolnych portów LAN	10
		Ogólna liczba przełączników poziomu dostępowego	1
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#27 Radioterapia		
		Ogólna liczba portów LAN	32
		Liczba zajętych portów LAN	25
		Liczba wolnych portów LAN	7
		Ogólna liczba przełączników poziomu	2

		dostępowego	
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#28 Radioterapia_serwerownia		
		Ogólna liczba portów LAN	120
		Liczba zajętych portów LAN	66
		Liczba wolnych portów LAN	50
		Ogólna liczba przełączników poziomu dostępowego	3
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	1
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#29 Kuchnia		
		Ogólna liczba portów LAN	8
		Liczba zajętych portów LAN	6
		Liczba wolnych portów LAN	2
		Ogólna liczba przełączników poziomu dostępowego	1
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#30 Pralnia		
		Ogólna liczba portów LAN	8
		Liczba zajętych portów LAN	4
		Liczba wolnych portów LAN	4
		Ogólna liczba przełączników poziomu dostępowego	1
		Ogólna liczba przełączników poziomu	0

		szkieletowego	
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#31 Patomorfologia		
		Ogólna liczba portów LAN	24
		Liczba zajętych portów LAN	12
		Liczba wolnych portów LAN	12
		Ogólna liczba przełaczników poziomu dostępowego	1
		Ogólna liczba przełaczników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#32 Centrala Tel		
		Ogólna liczba portów LAN	48
		Liczba zajętych portów LAN	13
		Liczba wolnych portów LAN	35
		Ogólna liczba przełaczników poziomu dostępowego	2
		Ogólna liczba przełaczników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#33 Dział Techniczny		
		Ogólna liczba portów LAN	32
		Liczba zajętych portów LAN	22
		Liczba wolnych portów LAN	10
		Ogólna liczba przełaczników poziomu dostępowego	2
		Ogólna liczba przełaczników poziomu szkieletowego	0
		Ogólna liczba routerów	0

		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#34 Psych_parter		
		Ogólna liczba portów LAN	72
		Liczba zajętych portów LAN	45
		Liczba wolnych portów LAN	27
		Ogólna liczba przełaczników poziomu dostępowego	2
		Ogólna liczba przełaczników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#35 Psych_1		
		Ogólna liczba portów LAN	72
		Liczba zajętych portów LAN	32
		Liczba wolnych portów LAN	40
		Ogólna liczba przełaczników poziomu dostępowego	2
		Ogólna liczba przełaczników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#36 Psych_2		
		Ogólna liczba portów LAN	72
		Liczba zajętych portów LAN	26
		Liczba wolnych portów LAN	46
		Ogólna liczba przełaczników poziomu dostępowego	2
		Ogólna liczba przełaczników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0

		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#37 Uzaleznienia_1		
		Ogólna liczba portów LAN	24
		Liczba zajętych portów LAN	12
		Liczba wolnych portów LAN	12
		Ogólna liczba przełaczników poziomu dostępowego	1
		Ogólna liczba przełaczników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#38 Uzaleznienia_2		
		Ogólna liczba portów LAN	8
		Liczba zajętych portów LAN	4
		Liczba wolnych portów LAN	4
		Ogólna liczba przełaczników poziomu dostępowego	1
		Ogólna liczba przełaczników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#39 Uzaleznienia_3		
		Ogólna liczba portów LAN	8
		Liczba zajętych portów LAN	7
		Liczba wolnych portów LAN	1
		Ogólna liczba przełaczników poziomu dostępowego	1
		Ogólna liczba przełaczników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0

8	#40 BOP		
		Ogólna liczba portów LAN	8
		Liczba zajętych portów LAN	3
		Liczba wolnych portów LAN	5
		Ogólna liczba przełączników poziomu dostępowego	1
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0
8	#41 A0_Rezonans		
		Ogólna liczba portów LAN	8
		Liczba zajętych portów LAN	6
		Liczba wolnych portów LAN	2
		Ogólna liczba przełączników poziomu dostępowego	1
		Ogólna liczba przełączników poziomu szkieletowego	0
		Ogólna liczba routerów	0
		Ogólna liczba urządzeń zabezpieczajacych typu firewall/UTM	0
		Ogólna liczba urządzeń zabezpieczajacych typu IDS/IPS	0

1.2.Serwerownia – stan obecny

Opis serwerowni	
1) Ilośc serwerowni	1
2) Systemy w serwerowni:	
a) ppoż (system czujek + centrala) (TAK/NIE)	czujka ppoż
b) ppoż (SUG) (TAK/NIE)	nie
3) klimatyzacja (TAK/NIE)	TAK
a) typ	Split 2 szt
b) wydajność	15kW
c) systsem kontroli parametrów pomieszczenia (TAK/NIE)	NIE
4) Szafy RACK	

a) ilość	3 stare + 2 nowe
b) Wypełnienie szaf (ile U wolnego miejsca zostało)	
c) czy jest miejsce pod dodatkowe szafy (TAK/NIE)	NIE
5) zasilanie awaryjne	
a) UPS (moc i wydajność - w znaczeniu czas podtrzymania pracy)	
b) agregat (dedykowany dla IT czy ogólny - opis)	
6) System prowadzenia kabli	brak podłogi technicznej, kable prowadzone w korytach ściennych lub luzem
7) inne wyposażenie serwerowni	
8) System kontroli dostępu	TAK
9) Opis pomieszczenia w ujęciu czy wymaga przeróbki (malowanie ścian, wymiana drzwi itp..)	zaślepienie drzwi z korytarza głównego

2. Przedmiot zamówienia

2.1. Opis przedsięwzięcia

Celem projektu jest uruchomienie nowej serwerowni dla systemów infrastruktury IT szpitala, w sposób taki aby zabezpieczyć działanie obecnej serwerowni, a w przyszłości przenieść obecnie funkcjonującą serwerownię do serwerowni budowanej. Celem projektu jest tez wdrożenie zaawansowanych systemów bezpieczeństwa, umożliwiających ochronę danych osobowych i danych medycznych istniejących w szpitalu oraz ochronę bazy danych.

Do wykonawcy będzie należało przede wszystkim wybudowanie nowej serwerowni od nowa w pomieszczeniach wskazanych przez Szpital, wraz z instalacjami niezbędnymi do jej funkcjonowania, wykonanie niezbędnego połączenia pomiędzy serwerownią nową i starą, wdrożenie systemów zabezpieczeń IT oraz przeniesienie serwerów i macierzy do nowej serwerowni w sposób zapewniający dualizm rozwiązań. Do zadań wykonawcy będzie również należało uruchomienie nowej struktury sieciowej w szpitalu oraz zainstalowanie systemu WiFi.

Przedmiotem niniejszego zamówienia jest w szczególności:

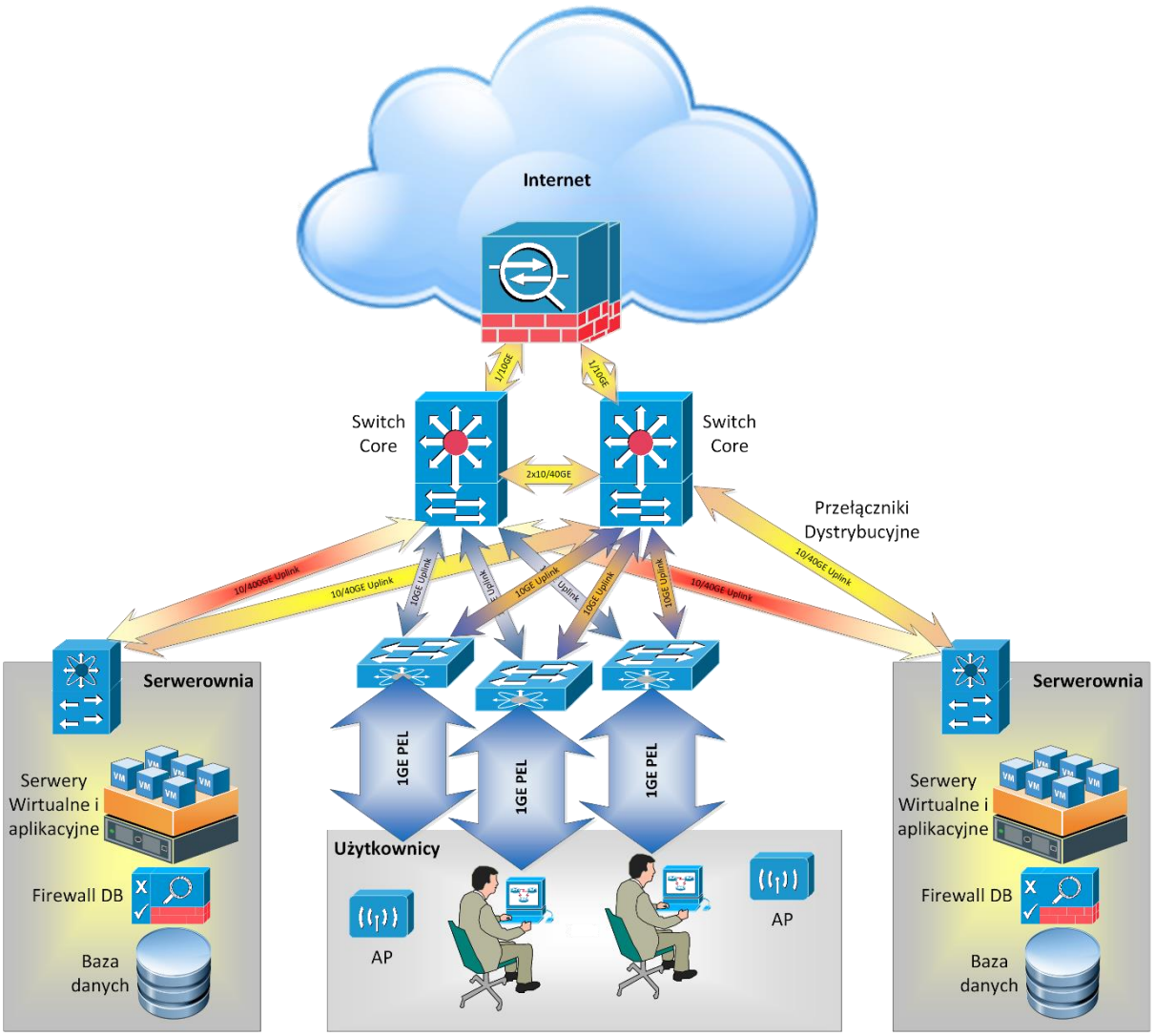
- Wykonanie i dostarczenie dokumentacji projektowej
- Budowa nowej serwerowni wraz z przyłączem energetycznym do wyłącznika głównego
- Dostawa, montaż i uruchomienie systemu klimatycznego
- Dostawa, montaż i uruchomienie systemu gaszenia
- Uruchomienie systemu nadzoru środowiskowego serwerowni
- Dostawa i montaż okablowania strukturalnego
- Dostawa, montaż i uruchomienie punktów dostępowych sieci WiFi
- Dostawa, montaż i uruchomienie nowych zasobów sieciowych
- Dostawa, montaż i uruchomienie systemu bezpieczeństwa informatycznego
- Przeniesienie sprzętu ze starej serwerowni do nowej.

- Testy i uruchomienie
- Szkolenia
- Odbiór końcowy oraz rozpoczęcie świadczenia usług serwisowych.

2.2. Docelowa architektura infrastruktury

System informatyczny od strony sieciowej będzie skonfigurowany w postaci gwiazdy, tj. każdy z przełączników dostępowych będzie połączony z dwoma urządzeniami szkieletowymi dwoma linkami, w przypadku awarii jednego przełącznika lub jednego linku będzie dostępny drugi. Urządzenia i połączenia szkieletowe i agregacyjne będą docelowo wzajemnie się duplikowały. Łączność z urządzeniem końcowym klienckim – komputerem czy urządzeniem medycznym, będzie wykonany już pojedynczym połączeniem miedzianym. Kontakt z urządzeniem sieciowym sieci bezprzewodowej również będzie wykonany pojedynczym linkiem ale redundancja połączeń bezprzewodowych będzie wynikała w paśmie radiowym, tj. urządzenia będą zachodzić zasięgiem na siebie. Będzie to wynikało z planowania radiowego, które zostanie wykonane przed wdrożeniem. Połączenia z urządzeniami serwerowymi będą wykonywane w serwerowni minimum dwoma uplinkami do przynajmniej dwóch urządzeń dostępowych – serwerowych. Awaria połączenia, karty czy switcha nie wyeliminuje łączności. Poza tym połączenia takie będą zagregowane czyli będą działały z podwójna prędkością. Połączenia z UTM infrastruktury będą się odbywały minimum 4 uplinkami z przełączników serwerowych. UTM będzie miał połączenie z siecią Internet, oraz poprzez VPN z siecią bezpośrednio poprzez WAN (np. link ciemnego światłowodu) i VPN poprzez Internet.

Szczegóły połączeń są zobrazowane na rysunku poniżej.

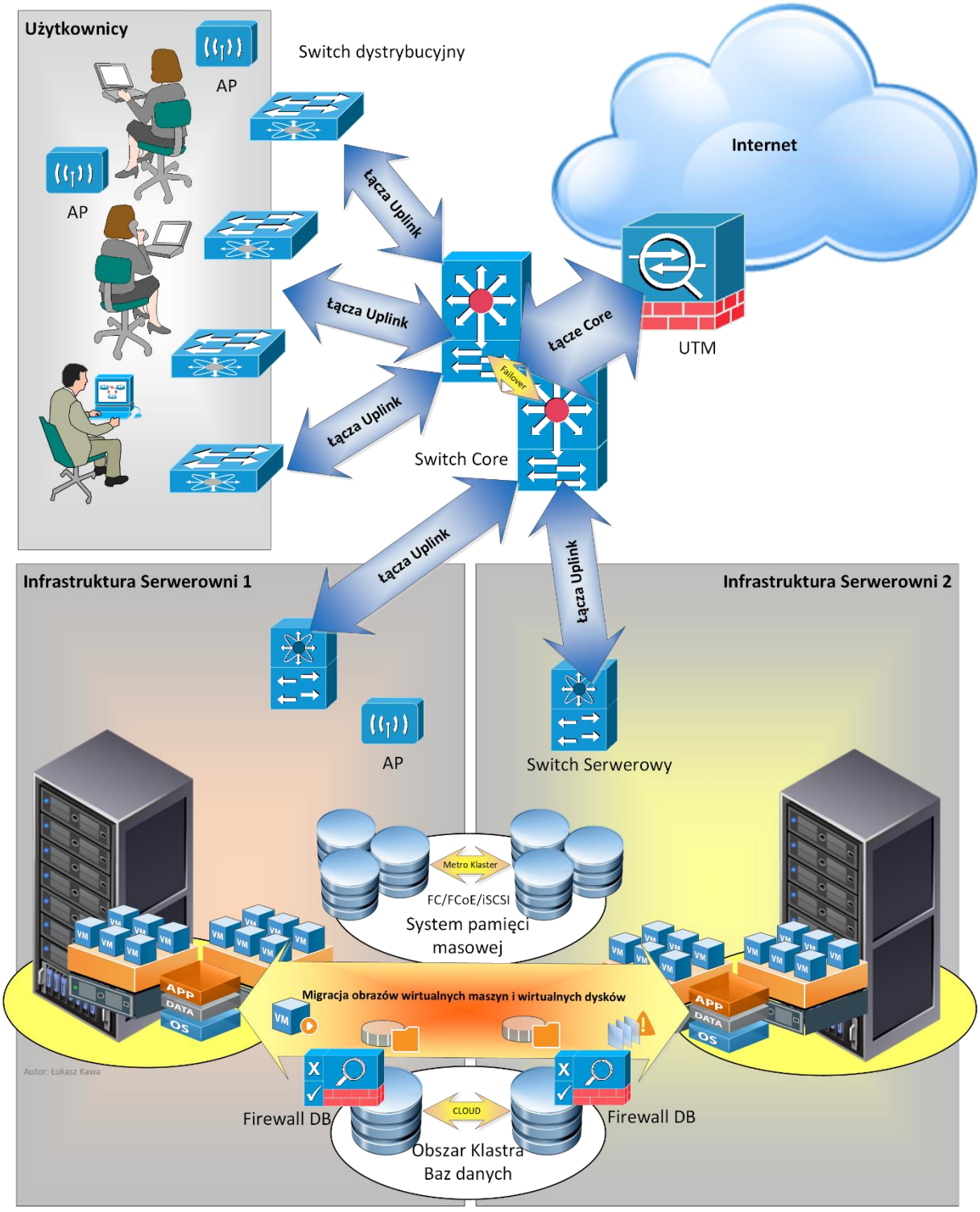


Rysunek 1 Szczegóły połączeń architektury sieciowej

Szpital obecna serwerownie rozbuduje o drugą i będzie posiadał dwie serwerownie fizyczne. Oznacza to, że jeżeli szpital będzie posiadał urządzenia dla drugiej serwerowni ale w odrębnej szafie RACK, będzie to dla infrastruktury urządzenie klasy DR – Disaster Recovery ale w tym samym pomieszczeniu. Tam gdzie to możliwe sugeruje się oddzielenie serwerowni od siebie. Sprzęt serwerowy taki jak Serwery, macierze czy sprzęt rdzenia sieci zostanie umieszczony w każdej serwerowni lub w każdej szafie oddzielnie. Całość zostanie zasilona bezpośrednim połączeniem prądowym 0,4kV z przyłącza głównego szpitala.

Szczegóły rozmieszczenia logicznego w serwerowni.

Szacuje się, że urządzenia nowe zastąpią urządzenia stare lub je uzupełnią. W tym wypadku aby nie mnożyć infrastruktury serwerów fizycznych, należy zainstalować obszar wirtualizacji serwerów, a serwery do tej pory wykorzystywane jako serwery stand-alone, należy przenieść w infrastrukturę wirtualną.



Rysunek 2 Architektura serwerowni

2.3. Zakres dostaw w zakresie serwerowni, okablowania, sprzętu informatycznego do zabezpieczeń danych

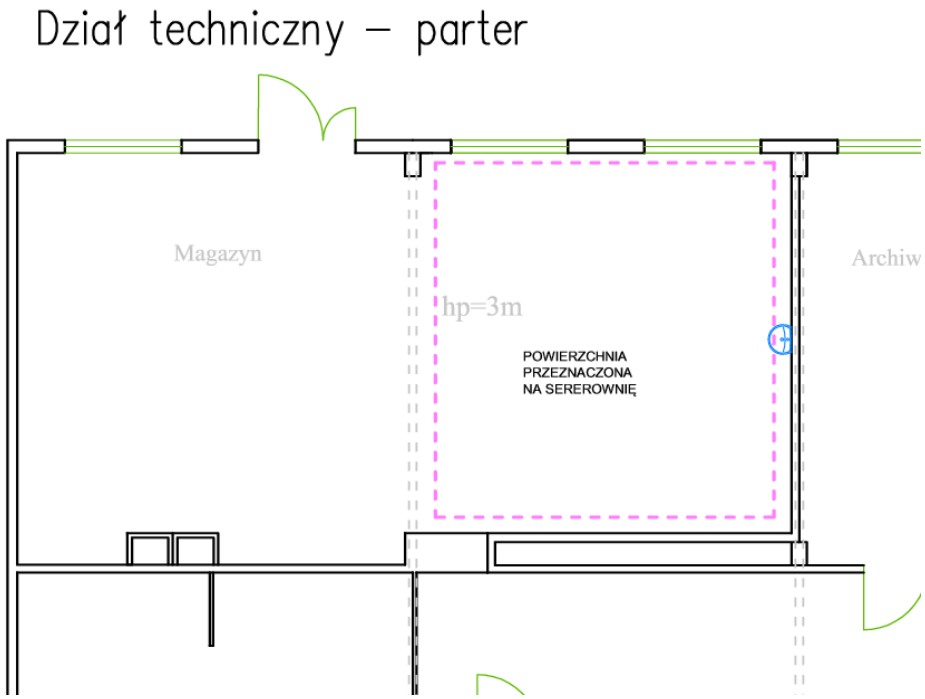
Tabela 1Tabela realizacji

Lp.	Opis głównych parametrów technicznych	Ilości minimalne	Jednostka miary
1.	Budowa serwerowni – prace budowlane i wykończeniowe (w tym drzwi p.poż)	1	kpl.
2.	Prace budowlane w branży elektrycznej (w tym montaż rozdzielni elektrycznej i kabla zasilającego)	1	kpl.
3.	Dostawa i montaż UPS 10kW	2	szt.
4.	Wykonanie systemu SUG	1	kpl.
5.	Wykonanie systemu SSWiN i p.poż	1	szt.
6.	Prace budowlane dot. systemu klimatyzacji i wentylacji (wraz z dostawą i montażem wyposażenia)	1	kpl.
7.	Szafy RACK	3	szt.
8.	Wykonanie połączenia światłowodowego z obecną serwerownią (96j)	1	szt.
	Wykonanie połączeń światłowodowych z PD i WiFi	40	szt.
	Wykonanie połączeń sieciowych z urządzeniami WiFi	40	szt.
	Switch dostępowy PoE	40	szt.
	Moduły SFP+ 10Gb/s (z odpowiednimi kablami krosowymi)	160	szt.
	Punkty dostępowe WiFi	40	szt.
	UTM	1	szt.
	Urządzenie bezpieczeństwa danych	1	kpl.

3. Parametry minimalne dla dostaw w zakresie serwerowni, okablowania, sprzętu informatycznego oraz systemów medycznych

3.1 Opis prac budowlano- instalacyjnych w zakresie przebudowy pomieszczeń na potrzeby serwerowni

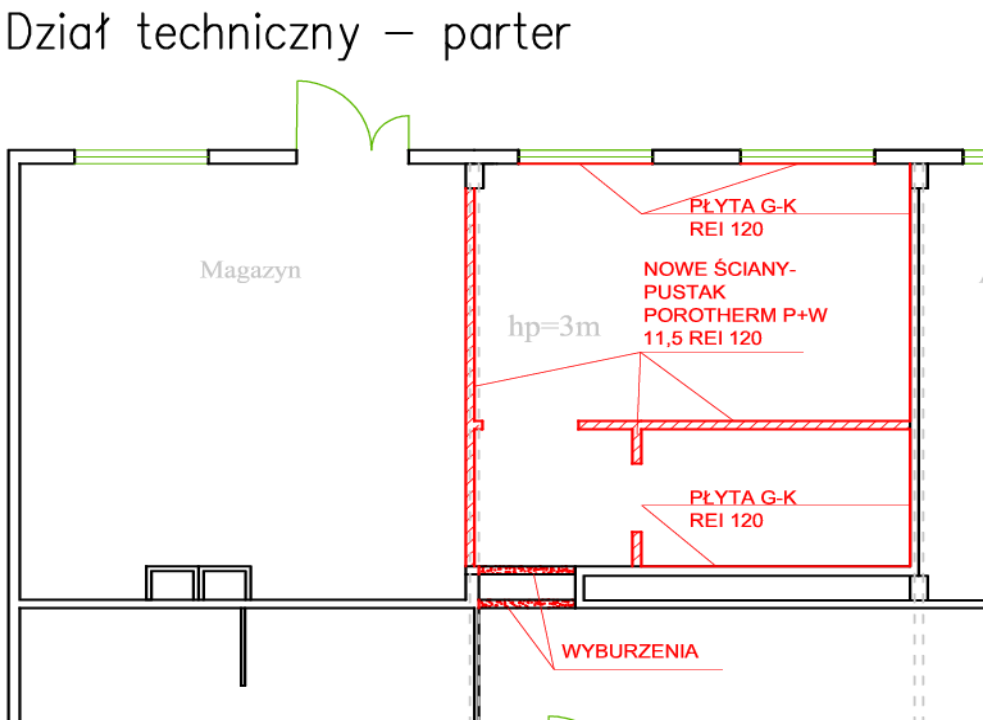
Istniejące pomieszczenie wykorzystywane jest obecnie jako pomieszczenie magazynowe. Posadzka w pomieszczeniu wykonana jest z płytek ceramicznych z zastosowaniem podkładu izolującego z gumy. Sufit i ściany tynkowane malowane. Okna zabezpieczone są od zewnątrz kratami. W pomieszczeniu zainstalowane są urządzenia elektryczne i teletechniczne. W celu dostosowania pomieszczenia do nowoprojektowanej funkcji konieczne przewiduje się zamurowanie i wydzielenie odrębnego pomieszczenia. Poziom posadzki w pomieszczeniach objętych opracowaniem zostaje zachowany.



Zakres prac obejmuje m. innymi:

- demontaż starych okładzin ściennych i podłogowych,
- demontaż instalacji elektrycznych i teletechnicznych,
- demontaż instalacji sanitarnych (wod kan, co)
- wyburzenie części ścian działowych,
- skucie wylewek cementowych (jeżeli będzie konieczne),

- wymurowanie nowych ścian działowych,
- wykonanie nowych nadproży w otworach drzwiowych,
- wykonanie nowych wylewek cementowych,
- wykonanie nowych przekuć do instalacji wentylacji(w uzgodnieniu z konstruktorem),
- wykonanie nowej instalacji elektrycznej,
- wykonanie instalacji przeciwpożarowej,
- wykonanie instalacji wentylacji mechanicznej oraz instalacji klimatyzacji,
- wykonanie instalacji freonowych, odpływu skroplin, montaż i uruchomienie klimatyzatorów,
- montaż stolarki drzwiowej,
- montaż drzwi p.poż.,
- wykonanie nowych okładzin ściennych i podłogowych,
- montaż gniazd wtykowych, itp.
- wyposażenie pomieszczeń,
- oznakowanie pomieszczeń.



Serwerownie należy wyposażyć w systemy i urządzenia:

- Dedykowane szafy serwerowe typu RACK,

- Dedykowane zasilacze awaryjne UPS,

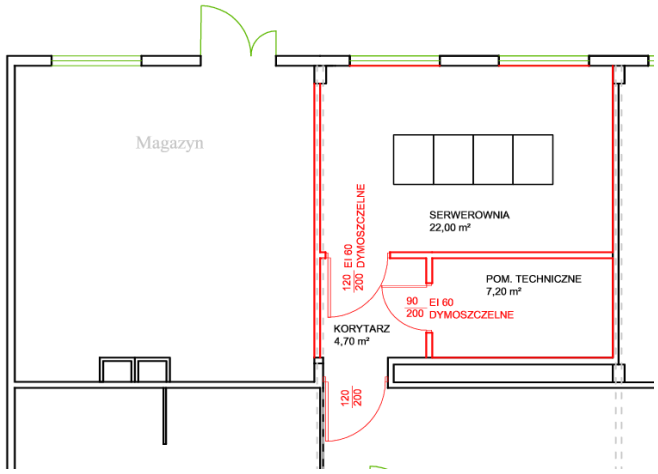
- Okablowanie strukturalne LAN,

- System kontroli dostępu, instalacja Wi-Fi

- System monitoringu parametrów urządzeń.

Pomieszczenie serwerowni należy wyposażyć w systemem koryt kablowych do rozprowadzenia instalacji elektrycznej i teleinformatycznej.

Dział techniczny – parter



Przy realizacji zadania Wykonawca zastosuje materiały i urządzenia nowe, dopuszczalne do obrotu i stosowania w obiektach użyteczności publicznej oraz pełnowartościowe, tj. I gat., dla których wydano odpowiednie świadectwa i certyfikaty, atesty, aprobaty techniczne lub inne deklaracje zgodności. Użyte materiały budowlane, instalacyjne i wykończeniowe oraz wyposażenie muszą zapewnić niskie koszty eksploatacji, przy narzuconym przez Zamawiającego standardu wykończenia i użytkowania. Od Wykonawcy wymagać się będzie przedstawienia wymaganych atestów, certyfikatów oraz deklaracji zgodności z Polskimi Normami lub Aprobatami Technicznymi na zastosowane materiały, wyroby. Dostarczane przez Wykonawcę na teren budowy materiały i urządzenia muszą uzyskać akceptację Zamawiającego pod względem funkcjonalnym, trwałości użytkowania, estetycznym i kolorystyki.

3.1.1. Wytyczne branży budowlanej

Pomieszczenie serwerowni wraz z pomieszczeniami towarzyszącymi należy wykonać wg standardów stawianych dla ww. pomieszczeń technicznych. Przedmiotowe pomieszczenia powinny posiadać nośność posadzki 1500 kg/m2 i być pozbawione instalacji innych, niż dedykowanych dla funkcjonowania serwerowni.

Zastosować:

a) ściany z bloczków z betonu komórkowego lub sylikatów

b) nadproża systemowe
c) tynki cementowo – wapienne kat. IV, charakteryzujące się bardzo dobrą techniką wykonania bez widocznych śladów uchybień, gładkie i wytrzymałe na uszkodzenia mechaniczne,
d) drzwi wejściowe należy wyposażyć w system kontroli dostępu używany przez Zamawiającego.
e) ślusarka aluminiowa wewnętrzna w kolorze RAL 7030, zgodne z wymaganiami p. poż.
f) wykładzina podłogowa PCV homogeniczna, wykładzina prądoprzewodząca, zapewniająca właściwe odprowadzanie ładunków elektrostatycznych z całej powierzchni podłogi, grubość całkowita min. 2 mm, klasa ścieralności T, odporność ogniowa B-s1, klasa użyteczności 34/43, bez konieczności akrylowania /ponownej konserwacji polimerami przez cały okres użytkowania, kolorystyka jasna z minimalną ilością bezkierunkowego wzoru, nowoczesne wzornictwo. Posadzki z wykładziny PCV wywinąć na ścianę na wysokość 15 cm. Możliwość łączenia w danym pomieszczeniu kilku wzorów (kolorów).
g) wykładzina ścienna PCV homogeniczna, grubość całkowita min.1,2 mm, grubość warstwy użytkowej min. 1,2 mm na wysokość 1m powyżej wywinięcia wykładziny podłogowej, ochrona wszystkich ścian wykładziną PCV do wysokości min. 1m od wywinięcia posadzki.
h) narożniki wypukłe zabezpieczyć narożnikiem ochronnym systemowym.
i) malowanie farba lateksowa, malowanie dwukrotne. Charakterystyka farby: łatwo zmywalna, nie brudząca się, odporna na preparaty czyszczące, matowienie. Kolorystyka do uzgodnienia z Zamawiającym.
j) Wszystkie materiały i elementy wykończeniowe pomieszczeń należy uzgodnić z Zamawiającym na etapie projektowania.

3.1.2. Instalacja wod.- kan -c.o.

Wszystkie instalacje wodne (podejścia do jednej umywalki i kurka czerpalnego) należy zdemontować, zakorkować skutecznie poza obrębem pomieszczeń serwerowni.

W związku z nową aranżacją pomieszczeń należy zdemontować dwa grzejniki, a przewody doprowadzające c.o. zakorkować skutecznie poza obrębem pomieszczeń serwerowni.

3.1.3. Instalacja elektryczna

Zapotrzebowanie mocy dla istniejących oraz projektowanych urządzeń zlokalizowanych w przebudowanej serwerowni oraz pozostałych urządzeń, w tym chłodniczych, nie powinno przekroczyć 30kW. W pomieszczeniu technicznym serwerowni należy zlokalizować rozdzielnice elektryczną serwerowni RS 0,4kV dwustronnie zasilaną nowoprojektowanymi liniami kablowymi 0,4kV oraz UPS-y. Rozdzielnice RS, wyposażyć w układ automatycznego przełączenia zasilania (APZ). UPS-y zasilić z rozdzielnicy RS. Nowa serwerownia będzie połączona łączami teleinformatycznymi światłowodowymi z serwerami na budynku D oraz z planowaną serwerownią w planowanym budynku Bloku Operacyjnego.

Do szczegółowych uwarunkowań wykonania Przedmiotu zamówienia należy wykonanie dokumentacji projektowej oraz wszystkich prac budowlanych i instalacyjnych wraz z dostawą materiałów i urządzeń dotyczących wykonania serwerowni i pomieszczenia technicznego oraz układu zasilania, układu wentylacji i klimatyzacji, okablowania strukturalnego, kontroli dostępu oraz wizualizacji w szpitalnym systemie BMS. Zamówienie obejmować będzie kompleksową realizację, składającą się z następujących etapów procesu inwestycyjnego:

- Opracowanie dokumentacji projektowej,
- Wykonanie prac przygotowawczych, demontażowych i budowlanych we wszystkich pomieszczeniach, w których będą prowadzone prace,
- Wykonanie prac instalacyjnych w zakresie wymienionym w opisie,
- Dostawa materiałów i urządzeń,
- Uruchomienie urządzeń i wykonanie testów, pomiarów i badań sprawdzających, współdziałanie wszystkich zamontowanych i zainstalowanych elementów,
- Przeprowadzenie szkoleń personelu,
- Opracowanie dokumentacji powykonawczej w tym instrukcji obsługi i harmonogramu przeglądów serwisowych.

Dokumentację projektową, należy opracować zgodnie z ustawą z dnia 7 lipca 1994 – Prawo Budowlane (t.j. Dz. U. z 2010 r. nr 243 poz. 1623) oraz warunkami technicznymi wykonania i odbioru robót. Każda część dokumentacji powinna być podpisana przez projektanta z właściwymi uprawnieniami budowlanymi dla danej branży. Kompletną dokumentację projektową wraz z harmonogramem należy przedłożyć do zatwierdzenia. Wszystkie prace budowlano-instalacyjne prowadzone będą zgodnie z zatwierdzoną do realizacji dokumentacją projektową i harmonogramem.

Przedmiotowy opis, należy traktować jako zbiór założeń funkcjonalnych i minimalnych parametrów technicznych.

Ogólne założenia funkcjonalno-użytkowe

Wszystkie pomieszczenia należy wyposażyć w nową instalację oświetlenia podstawowego i awaryjnego (z możliwością wykorzystania istniejących) oraz instalację gniazd wtyczkowych LAN i 230V. Do zasilania rozdzielnicy serwerowni należy doprowadzić zasilanie podstawowe ze Stacji ST-1 NN sekcja II (około 80m) oraz zasilanie rezerwowane agregatem prądotwórczym ze stacji Agregatornia sekcja I (około 85m). Do zasilania elektrycznego serwerowni i klimatyzacji wykonać dedykowaną instalację elektryczną z rozdzielnicy elektrycznej serwerowni RS 0,4kV. W pomieszczeniu technicznym serwerowni należy zlokalizować rozdzielnice elektryczną RS 0,4kV dwustronnie zasilaną nowoprojektowanymi liniami kablowymi. Rozdzielnice RS wyposażyć w układ automatycznego przełączenia zasilania (APZ) z nastawianą zwłoką czasową. Układ zasilania energetycznego ma być pozbawiony pojedynczego punktu awarii poprzez zastosowanie podwójnego (niezależnego) zasilania do każdej szafy serwerowej. Zasilanie gwarantowane na potrzeby serwerowni zapewnią nowoprojektowane UPS-y, zasilane z rozdzielnicy RS. Szafy zlokalizować w serwerowni.

Wyłącznik główny do awaryjnego wyłączenia rozdzielni RS 0,4kV oraz zasilaczy UPS należy umieścić na przy wejściu głównym do budynku Działu Technicznego. Do klimatyzacji pomieszczeń należy wykonać instalację zgodnie z częścią branży instalacyjnej.

Pomieszczenia serwerowni wyposażyć w punkty serwisowe PEL (elektryczno-logiczne) i systemy elektronicznego nadzorowania i monitoringu (system kontroli dostępu, system monitoringu

parametrów urządzeń SMART GIRD) oraz wizualizacją we wskazanym pomieszczeniu na stanowiskach zdalnej obsługi serwerowni.

Drzwi wejściowe objąć kontrolą dostępu. Pomieszczenie musi być zabezpieczone pod względem elektrostatycznym. Przegrody budowlane otaczające pomieszczenie powinny mieć podwyższoną odporność ogniową EI60. Wszystkie przejścia instalacyjne zabezpieczyć do klasy odporności ogniowej przegród przez które przechodzą. Pomieszczenie powinno być pozbawione instalacji ciśnieniowych „obcych" w przypadku ich występowania, należy je zdemontować lub przebudować z pominięciem przebiegu w przedmiotowych pomieszczeniach. Oświetlenie podstawowe z użyciem opraw ze źródłami LED, kasetonowych 600x600mm z kloszem mlecznym. Natężenie oświetlenia ogólnego minimum 300-500Lx. Oświetlenie awaryjne zapasowe z użyciem opraw awaryjnych ze źródłami LED z funkcją autotestu z czasem potrzymania min 1h, posiadające aktualne świadectwo dopuszczenia CNBOP. Gniazda natynkowe serwisowe typu PEL (elektryczno-logiczne): 2x230V, 2x230V DATA, 2xRJ45 kat.6 w czterech narożnikach pomieszczenia. System koryt kablowych, układ i pojemność dostosowana do potrzeb z zapasem 100%, zapewniona separacja elektromagnetyczna dla instalacji elektrycznych i teleinformatycznych. W pomieszczeniu należy zapewnić wymagane dla serwerowni parametry temperatur, wentylacji oraz jakości powietrza. Serwerownia musi być wyposażona w zintegrowany system monitoringu warunków środowiskowych (temperatura, wilgotność) - system musi umożliwiać wyświetlanie aktualnych wyników pomiaru na wyświetlaczu oraz mieć możliwość powiadamiania po wystąpieniu alarmu poprzez email. Zasilanie prowadzone w układzie redundantnym i dwutorowym do każdej z szaf Rack serwerowych i sieciowych. Z rozdzielnicy napięcia gwarantowanego RS wykonać zasilanie do listew zasilających w szafach serwerowych i sieciowych. Kable dobrać do zakładanych obciążeń wg norm. Serwerownia musi być wyposażona w zintegrowany system ESO - kontrola dostępu (parametry techniczne do uzgodnienia z Zamawiającym) oraz w system telewizji dozorowej. Instalację elektryczną oświetlenia oraz gniazd elektrycznych prowadzić natynkowo za pomocą kabli / przewodów bezhalogenowych układanych w rurach elektroinstalacyjnych niezapraszających dymu oraz szkodliwych gazów. W pomieszczeniu technicznym serwerowni lub w samej serwerowni (w zależności od przyjętego rozwiązania) planuje się ustawienie wiszącej rozdzielnicy elektrycznej RS 0,4kV w II klasie izolacji o stopniu ochrony min IP40 podzielonej na sekcję podstawową/rezerwową oraz gwarantowaną oraz centrale kontroli dostępu. Ponadto, w pomieszczeniu należy zapewnić swobodny dostęp do rozdzielnicy od frontu oraz do central kontroli dostępu.

Źródłem zasilania podstawowego i rezerwowego będą istniejące rozdzielnice główne RG 0,4kV. Przedmiotowe rozdzielnie stanowią infrastrukturę własną Inwestora/Zamawiającego.

Szczegółowe wymagania dla zasilania podstawowego i rezerwowego:

• Rozbudowa rozdzielnicy głównej zasilania podstawowego i rezerwowego o dodatkową aparaturą zabezpieczającą wyłącznikami mocy typu „compact" z regulacją prądu zabezpieczenia linii zasilającej.

• Do zasilania stosować kable miedziane.

• Linie kablowe prowadzone w rurociągu kablowym, rury typu HDPE dwuwarstwowe karbowane i w budynkach w dedykowanych korytach kablowych.

Wymagania dla systemu uziemień i połączeń wyrównawczych.

• W serwerowni wymagany jest uziom otokowy,

• Dla potrzeb serwerowni wykonać nowe uziemienie, taśma stalowa FeZn 30x4

• Nowy uziom, połączyć z główną szyną wyrównawczą budynku

• Wartość rezystancji uziemienia maksymalnie 5 Ω

• Połączenia wyrównawcze między wszystkimi elementami przewodzącymi obcymi, linką LgYżo 16mm2

Wymagania dla oświetlenia podstawowego i awaryjnego

• Natężenie oświetlenia podstawowego w serwerowni minimum 300lx w każdym punkcie

• Natężenie oświetlenia awaryjnego (zapasowe) minimum 30lx każdym punkcie

• Oprawy systemowe do sufitów podwieszanych kasetonowych o wymiarze 600x600mm

• Oprawy oświetlenia podstawowego ze źródłami światła w technologii LED z kloszem mlecznym, wymiar 600x600mm

• Oprawy oświetlenia awaryjnego punktowe ze źródłami światła w technologii LED z czasem podtrzymania oświetlenia awaryjnego min. 1-godzina

Wymagania dla systemu koryt kablowych

• Koryta siatkowe z prętów stalowych ocynkowanych galwanicznie

• Dostępne rozmiary o szerokości od 50mm do 300mm i wysokości min. 50mm

• Zawiesia systemowe dostosowane do przekroju koryt

• Przekrój koryt dobrany z zapasem min. 50%

Wymagania dla układu zasilania energetycznego serwerowni

• Zasilanie dwutorowe (podstawowe i rezerwowe) z zachowaniem wymagań Tier III,

• Układ rozdzielni trzy polowy:

- pole zasilające z układem automatycznego załączania rezerwy SZR

- pole odpływowe podstawowe/rezerwowe

- pole odpływowe gwarantowane

• Układ automatycznego przełączania źródła zasilania w czasie krótszym niż 90 sekund

• Rozdzielnie elektryczne na prąd 250A i napięcie 400V

• Wymiary szaf 800-1200x400x1400mm (szerokość x głębokość x wysokość)

• Konstrukcja szaf skręcana z profili stalowych

• Aparaty główne i odpływowe z zabezpieczeniem torów fazowych i neutralnego

• Punkt PE rozdzielni połączony z szyną uziemiającą

• Kable zasilające do rozdzielni do układania na stałe typu YnKY, napięcie izolacji 0,6/1kV, przekrój dobrany do obciążalności prądowej i maksymalnych dopuszczalnych spadków napięcia lub wg wytycznych producenta/dostawcy podłączanych urządzeń

• Kable zasilające do zasilaczy awaryjnych UPS i szaf serwerowych giętkie typu JZ-750, napięcie izolacji 0,6/1kV, przekrój dobrany do obciążalności prądowej i maksymalnych dopuszczalnych spadków napięcia lub wg wytycznych producenta/dostawcy podłączanych urządzeń

• Układ zasilania powinien być wyposażony w zdalny wyłącznik awaryjny zlokalizowany na zewnątrz przy wejściu do budynku

• Rozdzielnia zasilania podstawowego i awaryjnego powinna być wyposażona w układ pomiarowy parametrów zasilania: moc, prąd i napięcie, wyposażony w wyświetlacz LCD i możliwością zdalnego odczytu, komunikacja

3.1.4. Dostawa i instalacja UPS

CECHA	MINIMALNE WYMAGANIA TECHNICZNE
Moc znamionowa	Min. 10kVA / 9kW (PF=0,9)
Topologia	online VFI-SS-111
Architektura	UPS konwencjonalny posiadający wewnętrznie zduplikowane zasilacze elementów sterujących
Sprawność energetyczna	do 95% całkowita w trybie przetwarzania VFI do 98,5% w trybie ekonomicznym
Fazy wej. / wyj.	3/3
Napięcie wejściowe	400V w układzie trójfazowym z możliwością regulacji napięcia wejściowego jak poniżej
Zakres napięcia wejściowego	208/467 V (50%) / 312-467 V (100%)
Częstotliwość wejściowa	45-65Hz
THDi	< 5% / pełne obciążenie
Wejściowy współczynnik mocy (PF)	> 0,99
Napięcie wyjściowe	380, 400, 415V, 50/60Hz
Tolerancja napięcia wyjściowego	± 1%
THDu	2%
Crest Factor	3 : 1 zgodnie z EN62040-3
Przeciążenie falownika	150% / 60s, 125% / 10 min.

Współpraca ze źródłem (sieć / agregat)	Tak
Czas autonomii	Min. 10 min. przy obciążeniu 70% (baterie koniecznie w szafie z elektroniką UPS, pomiar temperatury baterii, falownika i prostownika – jako oddzielne układy)
Typ baterii	Szczelne, bezobsługowe (VRLA), 7 lub 9Ah
Żywotność wg Eurobat	6-9 lat (przy 20°C)
Układ mechaniczny	Moduły bateryjne w postaci wymiennych szuflad umieszczone w szafie systemowej UPSa
Charakterystyka ładowania	Ładowanie zaawansowane forsujące oraz utrwalającego
Prąd ładowania baterii	Min. 3A
Bypass	wbudowany automatyczny / serwisowy
Zintegrowany centralny ręczny bypass serwisowy dla całego systemu	tak
Panel Użytkownika	Panel dotykowy TFT lub ciekłokrystaliczny 3,5”, konfiguracja zabezpieczana hasłem
Porty komunikacyjne	· Min. 1 x RS-232 / RS-485 · Min. 4 styki beznapięciowe (ustawienie domyślne: normalnie otwarte) · E.P.O. (wył. ppoż.) – konfigurowalne NO/NC z panelu dotykowego Styki zabezpieczenia przez prądem wstecznym NO/NC
Zdalna komunikacja / monitoring	Adapter SNMP typu „plug-in”
Obsługa serwisowa UPSa	Dostęp serwisowy od boków i przodu urządzenia
Sposób podłączenia wejścia / wyjścia	Zaciski na szynie omega z przodu i od dołu UPSa
Chłodzenie	Wymuszone (wentylatory z automatyczną kontrolą prędkości obrotowej)
Temperatura pracy	0°C - 40°C
Wilgotność względna	20% - 95% bez kondensacji
Normy	EN 62040-1, EN 62040-2, EN 62040-3, CE, ISO 9001

3.1.5. Wykonanie systemu KD, SSWiN oraz monitoring parametrów środowiskowych oraz stanu pracy.

1. Pomieszczenie serwerowni należy wyposażyć w system Kontroli Dostępu (KD) oraz System Sygnalizacji Włamania i Napadu (SSWiN).
2. System kontroli dostępu należy zrealizować w oparciu o centralę alarmową oraz czytniki kart zbliżeniowych umieszczony przy drzwiach wejściowych do pomieszczenia serwerowni. Zabezpieczenie dostępu do serwerowni należy zrealizować poprzez rozbudowę posiadanego systemu firmy AutoID.
3. Pomieszczenie trzeba wyposażyć w kontroler Virdi MCP-040 oraz czytniki kart zbliżeniowych RFID.
4. Dla celów bezpieczeństwa przy wyjściu z pomieszczenia serwerowni zainstalować należy awaryjny przycisk wyjścia umożliwiający otwarcie przejścia nawet w przypadku uszkodzenia kontrolera lub czytnika.
5. System sygnalizacji włamania i napadu (SSWiN) w celu wykrycia nieuprawnionego wejścia do serwerowni. W przypadku, kiedy uda się w jakiś sposób "obejść" system kontroli dostępu, instalacja SSWiN zidentyfikuje takie zdarzenia przy pomocy odpowiednich sensorów (kontaktron w drzwiach, czujki ruchu itp.). Zdarzenie zostanie zasygnalizowane (w sposób optyczny i akustyczny) za pomocą sygnalizatora oraz, przy odpowiedniej konfiguracji, powiadomione zostaną automatycznie o zdarzeniu wskazane osoby lub służby.
6. System SSWiN powinien składać się poniższych elementów:
   a) centrali alarmowej,
   b) pasywnych czujek podczerwieni,
   c) akustycznej czujki stłuczenia szyb,
   d) czujek magnetycznych stykowych (kontaktrony) umożliwiających wykrywanie,
   e) działania związanego z otwarciem drzwi i okien,
   f) akustyczno – optycznych sygnalizatorów alarmu,
   g) modułów komunikacyjnych.

3.1.6. Wykonanie systemu SSP i SUG

System sygnalizacji pożaru w budynku SSP

Obiekt zalicza się do grupy niskie oraz do kategorii zagrożenia ludzi ZL III plus PM.

Podział obiektu na strefy pożarowe: Należy wydzielić pożarowo pomieszczenia Serwerowni, w tym oddzielnie pomieszczenie serwerowe i oddzielnie pomieszczenie UPS.

Kable elektryczne w miejscach przebić ścian i stropów oddzielenia przeciwpożarowego muszą być odpowiednio zabezpieczone przed przenoszeniem pożaru, za pomocą atestowanych środków technicznych.

Przepusty instalacyjne o średnicy większej niż 4 cm, przechodzące przez stropy między kondygnacjami powinny mieć klasę odporności ogniowej EI 60.

UWAGA: W budynku należy uwzględnić projekt SSP opracowany przez firmę CERBEX p/n „Rozbudowa instalacji systemu sygnalizacji pożaru i budowa instalacji dźwiękowego systemu ostrzegawczego w Szpitalu Wojewódzkim im. Św. Łukasza SP ZOZ w Tarnowie” (rysunek SSP 2.1, 2.2, 0.1.

Projekt systemu Sygnalizacji Pożarowej jest w trakcie realizacji dla innych obiektów Szpitala. Należy zapoznać się z w/w dokumentacją i uwzględnić projektowane rozwiązania systemu p. poż. w całym Budynku Działu Technicznego. Dokumentacja projektowa powinna zostać zatwierdzona przez Rzeczoznawcę ds. Zabezpieczeń Przeciwpożarowych (zmiany usytuowania stref pożarowych). Zamawiający ma zainstalowany system sygnalizacji pożaru POLON 6000. System SSP należy wpiąć do centrali CSP 15 zlokalizowanej w Tunelu komunikacyjnym pomiędzy Działem Technicznym, a Budynkiem Kuchni.

Wykonanie systemu SUG

W pomieszczeniu Serwerowni należy zamontować stałe urządzenia gaśnicze wraz ze zbiornikiem/ zbiornikami ze środkiem gaśniczym.

Ochrona pomieszczania powinna odbywać się poprzez całkowite wypełnienie pomieszczenia chronionego gazem obojętnym.

Do ochrony pomieszczeń należy zastosować urządzenia sygnalizacji pożaru z centralą sterowania gaszeniem.

W skład systemu gaszącego w poszczególnych strefach wchodzą:

- centrala sterowania gaszeniem ,
- Bateria butli ze środkiem gaśniczym,
- rurociągi rozdzielcze i rozprowadzające,
- klapy odciążające,
- dysze rozprowadzające,
- Optyczne czujki dymu,
- Czujki zasysające z przewodami rozprowadzonymi wokół szaf ,
- ręczne przyciski:
  - START (uruchomienie),
  - STOP (zatrzymanie),
  - WSTRZYMANIE (blokada),
- sygnalizator ewakuacyjny,
- sygnalizator ostrzegawczy,
- inne wymagane.

Na wypadek awarii zasilania centrala CAG musi posiadać własne zasilanie rezerwowe i zostać podłączona do zasilania UPS.

Na terenie Szpitala zainstalowany jest SSP oparty na technologii POLON 6000. Do centrali SSP POLON należy przekazywać alarmy pożarowe wykryte serwerowni.

Zastosowane instalacje gaśnicze jak i system sterowania muszą posiadać aktualne dopuszczenia CNBOP.

3.1.7. Instalacja wentylacji i klimatyzacji

W ramach zamówienia należy wykonać dla powstającej serwerowni i pomieszczenia technicznego instalację chłodzenia z funkcją podmieszania powietrza świeżego. Pomieszczenia powinny posiadać

dwa niezależne systemy o podobnej wydajności, tak aby w razie awarii jednego systemu, drugi zapewnił równorzędne warunki mikroklimatu.

Klimatyzacją objąć należy następujące pomieszczenia:
- pomieszczenie techniczne / UPS
- serwerownia

Parametry doboru

Doboru instalacji należy wykonać dla następujących założeń

- docelowe zyski ciepła od serwerów: 20 kW
- temperatura powietrza wywiewanego: 28 °C
- temperatura powietrza nawiewanego: 14 °C

Kubatura pomieszczenia Serwerowni wynosi około 66m³ a Pomieszczenia technicznego około 22m³

Projektant instalacji obowiązany jest zorganizować obieg powietrza w taki sposób, aby przy temperaturze 32 °C powietrza wywiewanego przez centralę, nie pojawiały się komunikaty o przegrzewaniu się serwerów.

W celu doboru instalacji, należy przyjmować parametry zawarte w polskich normach, z wyjątkiem zewnętrznej temperatury w lecie, która powinna zostać przyjęta na poziomie 35 °C

W obliczeniach zysków ciepła pomieszczeń należy uwzględnić:
- zyski ciepła przez przegrody przezroczyste w wyniku nasłonecznienia i przenikania,
- zyski ciepła przez przegrody nieprzezroczyste z uwzględnieniem akumulacji ciepła,
- zyski ciepła związane dopływem powietrza zewnętrznego
- zyski lub straty ciepła przez przegrody sąsiadujących pomieszczeń,
- zyski ciepła i pary wodnej od ludzi,
- zyski ciepła od oświetlenia elektrycznego,
- zyski ciepła technologiczne od urządzeń,

Chłodzenie wodą lodową

Podstawowym sposobem chłodzenia pomieszczenia serwerowni powinna być centrala pobierająca powietrze z pomieszczenia kratkami wentylacyjnymi zlokalizowanymi pod stropem pomieszczenia ponad projektowaną lokalizacją serwerów oraz z pomieszczenia UPS. Powietrze będzie doprowadzane do centrali klimatyzacyjnej, gdzie będzie filtrowane z użyciem filtra F7 workowego o długości minimum 500mm, następnie powinno być ochładzane na chłodnicy wodnej zasilanej wodą lodową z sieci Szpitala. Centrala będzie nawiewała ochłodzone powietrze do pomieszczenia serwerowni oraz pomieszczenia UPS. Nawiew powietrza ochłodzonego powinien odbywać się przy użyciu jednego bądź kilku nawiewników wyporowych stojących na podłodze pomieszczenia i nawiewających powietrze do strefy korytarzowej lub regulowanych nawiewników umieszczonych w pobliżu szaf serwerowni. Górna krawędź nawiewników nie powinna być umieszczona wyżej niż 130cm.

Dodatkowo należy zapewnić podmieszanie powietrza zewnętrznego z istniejącej czerpni powietrza zewnętrznego doprowadzonej do pomieszczenia piwnicznego. Włączenie powietrza świeżego

powinno być wyposażone w klapę zwrotną oraz regulator stałego przepływu z możliwością nastawy od zewnątrz kanału.

Dopływ powietrza świeżego należy zapewnić na potrzeby higienicznej wentylacji pomieszczenia w ilości 0,5 wymiany godzinę, z możliwością regulacji.

Wypływ powietrza z pomieszczeń serwerowni będzie się odbywał nadciśnieniem z użyciem istniejącego kanału wentylacji grawitacyjnej, który należy doprowadzić do pomieszczenia serwerowni oraz UPS, należy również zapewnić wentylację ewentualnego przedsionka.

Układy zainstalować w Wentylatorni Działu Technicznego na poziomie piwnic. Do sterowania przepływem czynnika chłodniczego stosować zawór trójdrogowy z siłownikiem. Do chłodzenia należy wykorzystać wodę lodową o temperaturze 7/12 °C. W celu pozyskania wody lodowej należy wykonać wpięcie do głównego rurociągu w pomieszczeniu agregatornii a następnie wykonać rurociąg do Wentylatorni Działu Technicznego (odległość około 30m). Instalację wody lodowej wyposażyć w sprzęgło hydrauliczne z rozdzielaczem wyposażonym w trzy komplety króćców – jeden na potrzeby centrali klimatyzacyjnej oraz dwoma dodatkowymi - rezerwowymi. Rurociąg i sprzęgło wykonać z 50% zapasem przepływu.

Zgodnie z par.153 ust. 6. W.T. przewody powinny być wyposażone w otwory rewizyjne umożliwiające oczyszczenie wnętrza tych przewodów, a także innych urządzeń i elementów instalacji, o ile ich konstrukcja nie pozwala na czyszczenie w inny sposób niż poprzez te otwory, przy czym nie należy ich sytuować w pomieszczeniach o podwyższonych wymaganiach higienicznych.

Posadowienie central na wibroizolatorach lub podkładkach tłumiących i nieprzenoszących drgań, kanały wentylacyjne odizolować od drgań central wentylacyjnych kołnierzami elastycznymi. Przejścia przez ściany uszczelnione masami trwale plastycznymi. Na wlocie i wylocie z centrali zastosować tłumiki akustyczne kanałowe.

<u>Sterowanie centralą klimatyzacyjną</u>

Centrala klimatyzacyjna powinna być wyposażona w automatykę pozwalającą płynnie regulować temperaturą powietrza nawiewanego, temperaturą powietrza wywiewanego oraz wydajnością nawiewu.

Podstawowym sposobem regulacji będzie regulacja wydajności centrali - dla temperatury nawiewu powietrza na poziomie 20 °C, wydajność silnika powinna być regulowana w funkcji temperatury powietrza wywiewanego 28 °C.

Po osiągnięciu maksymalnej wydajności centrali, dalsza regulacja będzie realizowana poprzez programowe obniżenie poziomu zadanej temperatury powietrza nawiewanego dla zaworu regulacyjnego chłodnicy, alternatywnie możliwe jest przejście na regulacje zaworu w funkcji temperatury powietrza wywiewanego

W porozumieniu z Zamawiającym można zastosować inne procedury regulacji pod warunkiem zapewnienia oszczędności energii do zasilania wentylatorów i do chłodzenia. Wszystkie nastawy i zakresy użyte do regulacji muszą mieć możliwość edycji przez Użytkownika.

Należy zapewnić zapis parametrów pracy centrali.

Dodatkowe wymagania centrali

Należy stosować urządzenia cechujące się wysoką efektywnością energetyczną celem zapewnienia niskiego zużycia energii elektrycznej, tzn. wentylatory winny spełniać wymagania w zakresie współczynnika efektywności energetycznej określonego w Warunkach Technicznych, jakim powinny odpowiadać budynki i ich usytuowanie Dz.U.2002 r nr 75, poz.690 z późniejszymi zmianami.
Wentylator centrali powinien być typu EC, lub być sterowany falownikiem bądź być
Centrala powinna spełniać wymagania ERP tak jak dla central dla celów bytowych.

Właściwości obudowy centrali wynikające z normy PN-EN-1886:2008 lub równoważnej (potwierdzone certyfikatem TUV lub równoważnym)

- Szczelność obudowy:
  - przy podciśnieniu 400 Pa - klasa min L1
  - przy nadciśnieniu 700 Pa – klasa min L1
- Szczelność zamocowania filtra
  - przy podciśnieniu 400 Pa - klasa filtra 9
  - przy nadciśnieniu 400 Pa - klasa filtra 9
- Izolacyjność akustyczna obudowy – nie mniej niż 22dBA dla 250 Hz, nie mniej niż 30dBA dla 1000Hz.
- „Centrale wentylacyjne muszą spełniać ROZPORZĄDZENIE KOMISJI (UE) NR 1253/2014 z dnia 7 lipca 2014 r. w sprawie wykonania Dyrektywy Parlamentu Europejskiego i Rady 2009/125/WE w odniesieniu do wymogów dotyczących Ekoprojektu dla systemów wentylacyjnych obowiązujących od 01.01.2018r.”
- Konfiguracja central musi zapewnić możliwość inspekcji oraz czyszczenia wymienników bez konieczności ich demontażu.
- Taca ociekowa pod chłodnicą wykonana z jednostronnym lub dwustronnym spadkiem, zapewniające stały i swobodny spływ kondensatu. Nie dopuszcza się aby kondensat zaległ w centrali. Odprowadzenie skroplin poprzez syfon antyzapachowy.
- Okno inspekcyjne (średnica min 150 mm) w bloku wentylatora i filtra oraz oświetlenie typu LED.
- Filtr kieszeniowe o długości min 500 mm
- Chłodnica zaprojektowana jako stałoprzepływowa z pompą obiegową, sterowanie wydajnością z użyciem zaworu trójdrogowego z siłownikami.

Chłodzenie instalacją z bezpośrednim odparowaniem

Dodatkowym systemem chłodzenia będą klimatyzatory ścienne lub podstropowe. Należy zapewnić pełną redundancję względem centrali klimatyzacyjnej, czyli klimatyzatory powinny być dobrane na moc nie mniejszą niż chłodnica w centrali klimatyzacyjnej. W pomieszczeniu serwerowni należy zastosować przynajmniej dwa klimatyzatory skomunikowane ze sobą, które będą pracowały wymiennie. Należy zapewnić automatyczną okresową pracę urządzeń oraz komunikowanie awarii. Klimatyzatory powinny być dostosowane do chłodzenia w temperaturze - 30°C

Należy zastosować klimatyzatory z jednostką zewnętrzną ustawioną na dachu budynku, na stopach antywibracyjnych, urządzenia powinny posiadać następujące cechy:

- Agregaty skraplające winny być wyposażone w sprężarki inwerterowe.

- Urządzenia powinny być wyposażone w wentylatory z silnikami typu EC.
- Minimalna sprawność EER w trybie chłodzenia: 2,70
- Minimalna sprawność SEER w trybie chłodzenia: 6,2
- Klasa efektywności energetycznej w trybie chłodzenia: A++
- zakres pracy w trybie chłodzeniaz: -30 °C ~ 50 °C)
- Możliwość pracy naprzemiennej
- Możliwość komunikacji BMS (Modbus/BACnet)
- Port on/off
- Port alarmowy
- Detekcja wycieku czynnika chłodniczego
- Funkcja autodiagnozy
- Automatyczne uruchomienie po zaniku prądu bez utraty parametrów pracy
- Certyfikat PZH
- Certyfikat Eurovent

Wymagania ogólne dla sterowania

Zastosować dodatkowo pomiar temperatury w referencyjnym punkcie pomieszczenia, pomiar ten powinien być rejestrowany oraz mieć możliwość przypisania progów alarmu. Pomiar ten jest konieczny ze względu na konieczność kontroli temperatury również w razie wyłączenia centrali.

System sterowania powinien być niezależny od samej centrali i zachowywać pełną funkcjonalność w przypadku wyłączenia/awarii centrali lub systemu opartego na klimatyzatorach.

Zastosować zdecentralizowany układ sterowania (zabezpieczenie przed zatrzymaniem systemu w przypadku awarii pojedynczego elementu sterowania), posiadający komunikację w postaci dodatkowych informacji o stanach pracy urządzeń dla systemów powiadamiających oraz wizualizację w istniejącym w szpitalu systemie zarządzania budynkiem BMS(poprzez stosowane w Szpitalu protokoły komunikacyjne np. Modbus, S-Bus, BacNet)

Oklejenie szyb serwerowni

Szyby okien serwerowni należy okleić folią termoizolacyjną przeciwsłoneczną na całej powierzchni szyb. Oklejanie wykonać zgodnie z wytycznymi producenta folii.

Zastosować folię o następujących parametrach:

- przepuszczalności światła (VLT) nie większej niż 25%
- współczynnik redukcji energii słonecznej (TSER) nie mniejszej niż 80%

Wentylacja pożarowa

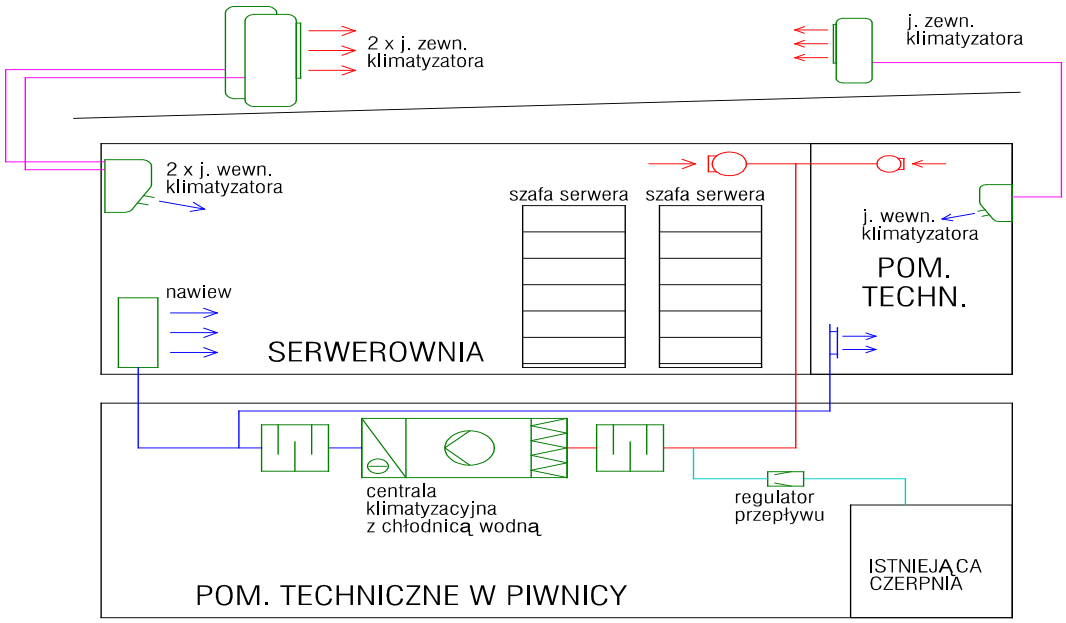
Budynek winien spełniać wymagania Warunków Technicznych jakim powinny odpowiadać budynki i ich usytuowanie (Dz. U.02.75.690), z późniejszymi zmianami w zakresie bezpieczeństwa pożarowego. Na etapie projektu budowlanego należy zweryfikować konieczność wykonania instalacji wentylacji pożarowej (oddymiającej) a w przypadku stwierdzenia takiej konieczności należy ją wykonać zgodnie z przywołanymi powyżej przepisami.

Założenia szczegółowe dla instalacji wentylacji, chłodzenia i klimatyzacji

Instalacja wentylacyjno-klimatyzacyjna ma za zadanie stworzyć właściwy mikroklimat dla obsługi technicznej i urządzeń pracujących w budynku. Instalacje wentylacyjne i klimatyzacyjne należy

wyposażyć w kompletne układy automatyki, dostarczyć do nich szafy rozdzielczo-sterownicze z okablowaniem sterowniczym i zasilającym od szaf do urządzeń. Dla pomieszczeń technicznych, w których dla zapewnienia właściwej pracy urządzeń konieczne jest odprowadzenie zysków ciepła i utrzymanie wymaganego zakresu temperatur.

Kanały rozprowadzające powietrze należy prowadzić w przestrzeni stropu podwieszonego lub w obudowach, w odpowiedniej izolacji termicznej i akustycznej.
Wszystkie przewody wykonać zgodnie z polskimi normami w klasie szczelności minimum B. Kanały wentylacyjne o przekrojach prostokątnych zaprojektować i wykonać jako gładkie z blachy stalowej o wysokiej odporności na korozję. Kanały wentylacyjne o przekrojach kołowych wykonać z rur i kształtek systemowych, z blachy stalowej ocynkowanej ze wzmocnioną powłoką antykorozyjną. Połączenia kołnierzowe kanałów wentylacyjnych wyposażyć w uszczelki na całej szerokości kołnierzy, nie wchodzące w światło kanału.
Wszystkie przewody wentylacyjne wyposażyć w odpowiednie otwory rewizyjne lub inne oraz miejsca dostępu do okresowego czyszczenia układów wentylacyjnych.
Na przejściach przez strefy pożarowe zainstalować klapy przeciwpożarowe sterowane elektrycznie (24V), łatwo dostępne do kontroli lub wymiany, włączone w system SSP szpitala.
Wszystkie otwory nawiewne i wywiewne klimatyzacji oraz wentylacji mechanicznej wyposażyć w urządzenia umożliwiające regulację ilości przepływającego powietrza.



3.1.8. Wymagania odnośnie dokumentacji projektowej i robót budowlano instalacyjnych

Warunki wykonania i odbioru prac projektowych

Przed przystąpieniem do opracowania projektu budowlanego niezbędne będzie wykonanie następujących opracowań:
- Szczegółowej inwentaryzacji pomieszczeń.

- Opracowanie niezbędnych ekspertyz i odstępstw wymaganych prawem.

Zamawiający będzie wymagał na etapie prac projektowych przedłożenia do akceptacji rysunków wykonawczych przed ich skierowaniem do realizacji.

Zakres prac projektowych obejmuje:

- wykonanie **projektu budowlanego wielobranżowego** z wymaganymi uzgodnieniami między innymi z rzeczoznawcą do spraw zabezpieczeń przeciwpożarowych, według obowiązujących przepisów prawa (jeżeli wymagane)

- wykonanie **dokumentacji projektowej wykonawczej wielobranżowej** w zakresie i formie, o której mowa w § 5 Rozporządzenia Ministra Infrastruktury z dnia 2 września 2004 r. w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego (tekst jednolity 2013 r. Dz. U. z 2013 r. poz. 1129);
- wykonanie **Specyfikacji Technicznych Wykonania i Odbioru Robót Budowlanych** przez którą należy rozumieć opracowania zawierające w szczególności zbiory wymagań, które są niezbędne do określenia standardu i jakości wykonania robót, w zakresie sposobu wykonania robót budowlanych, właściwości wyrobów budowlanych oraz oceny prawidłowości wykonania poszczególnych robót;
- **kosztorys inwestorski** w formie uproszczonej z uwzględnieniem wyposażenia;

Wykonawca dostarczy Zamawiającemu w/w kompletną dokumentację projektową ze wszystkimi wymaganymi uzgodnieniami w 4 egz. papierowych i 2 w wersji elektronicznej oraz dokumentację powykonawczą w ilości 2 egz. papierowe i 2 w wersji elektronicznej.

Warunki wykonania i odbioru prac budowlanych

Wykonawca zrealizuje zadanie inwestycyjne zgodnie z Programem Funkcjonalno –Użytkowym, opracowaną dokumentacją projektową, obowiązującymi przepisami prawa, zasadami wiedzy technicznej. Realizacja zadania, sprzęt budowlany i zakup materiałów leży po stronie Wykonawcy. Przy wykonywaniu robót należy uwzględniać instrukcje i zalecenia producenta wyrobów budowlanych co do ich zastosowania i montażu. W przypadku norm, atestów, aprobat technicznych nie wymienionych w niniejszym opracowaniu Wykonawca ma obowiązek stosować się do nich.

Prace instalacyjno– montażowe należy wykonać zgodnie z obowiązującymi przepisami.

Przy montażu instalacji kablowych i montażu urządzeń należy zwrócić szczególną uwagę na niżej podane sprawy:

· Wszystkie połączenia wykonać bardzo starannie, łączenie przewodów przez skręcanie i lutowanie lub na specjalnych zaciskach,
· Wykonać niezbędne pomiary elektryczne linii dozorowych i kablowych przed uruchomieniem systemu (m.in. pomiar rezystancji linii dozorowych, pomiar rezystancji izolacji, próby na przerwę i zwarcie),
· Montaż urządzeń wykonać w oparciu o dokumentację techniczno-ruchową,
· Zasilanie 230 V AC do centralek sygnalizacji pożaru, centralek automatycznego gaszenia pożaru oraz zasilacza ochrony pożarowej należy doprowadzić bezpośrednio z rozdzielni głównej (zasilanie z przed wyłącznika pożarowego).
· Przed przekazaniem systemu SAP i SUG Użytkownikowi, należy przeprowadzić rozruch wstępny wraz ze sprawdzeniem fizycznego zadziałania każdej czujki stosując odpowiednie urządzenia symulujące (dym, temperaturę, płomień) oraz wymagane protokoły rozruchowe.

Dokumentacja budowy

- Protokół przekazania terenu budowy
- Protokoły z narad i ustaleń
- Protokoły odbioru robót
- Dokumenty budowy należy starannie przechowywać i okazywać na życzenie Zamawiającego

Odbiorom podlegają zgłoszone Zamawiającemu zakończone etapy prac, robót i czynności, roboty zanikające i ulegające zakryciu, a także odbiór końcowy. Wykonawca jest zobowiązany do informowania Zamawiającego nie później niż na 3 dni przed zakryciem robót. Jeżeli Wykonawca nie poinformował o tych faktach Zamawiającego zobowiązany jest odkryć roboty lub wykonać odpowiednie odkrywki niezbędne do zbadania robót, a następnie przywrócić roboty do stanu poprzedniego, na swój koszt. Gotowość do odbiorów kolejnych etapów prac, robót określonych w harmonogramie rzeczowo-finansowym oraz robót ulegających zakryciu Kierownik Budowy zgłasza Zamawiającemu. Zamawiający ma obowiązek przystąpić do odbioru w terminie 7 dni, a w przypadku robót ulegających zakryciu 3 dni od daty zgłoszenia. Z czynności odbioru kolejnych etapów prac i robót sporządza się protokoły, zawierające opis przebiegu czynności danego odbioru oraz wszelkie ustalenia poczynione w jego toku. W przypadku stwierdzenia przy odbiorze wad i braków w wykonawstwie lub dokumentacji w stosunku do ich zamierzonego na dzień odbioru stanu, Zamawiający ma prawo odmówić odbioru i wyznaczyć termin do usunięcia tych wad.
Odbiór końcowy ma na celu przekazanie Zamawiającemu ustalonego przedmiotu umowy do eksploatacji Gotowość do odbioru końcowego Wykonawca zgłosi Zamawiającemu w formie pisemnej, a także przekaże Zamawiającemu całość wymaganej prawem dokumentacji powykonawczej.
Do odbioru końcowego Wykonawca jest zobowiązany przygotować następujące dokumenty:

- Dokumentację powykonawczą,
- Certyfikaty, deklaracje zgodności, aprobaty techniczne, świadectwa sanitarne wbudowanych materiałów,
- Instrukcje obsługi i użytkowania wszelkich urządzeń wyposażenia, schematy technologiczne, dokumentację techniczną, protokoły z pomiarów i rozruchu, instrukcję bezpieczeństwa eksploatacji, w tym instrukcję bezpieczeństwa pożarowego, itp.

Zamawiający przystąpi do odbioru końcowego w ciągu 7 dni od daty zgłoszenia zakończenia budowy przez Wykonawcę.
Zamawiający ma prawo odmówić odbioru, jeżeli w toku czynności odbioru zostanie stwierdzone, że przedmiot odbioru posiada wady, czynności lub nie zostały właściwie wykonane lub nie zostały przeprowadzone wszystkie sprawdzenia, próby, czy też niezbędne rozruchy technologiczne lub, gdy Wykonawca nie przedstawił wymaganych prawem i niezbędnych dokonania odbioru dokumentów powykonawczych lub przedmiot odbioru posiada inne usterki, uchybienia w stosunku do zamierzonego stanu.
Wykonawca zobowiązany jest do zawiadomienia na piśmie Zamawiającego o usunięciu wad oraz do żądania wyznaczenia terminu odbioru zakwestionowanych uprzednio robót jako wadliwych.
Zamawiający sporządzi protokół z odbioru końcowego podpisany przez strony postępowania.
Zamawiający wyznaczy datę gwarancyjnego odbioru robót przed upływem terminu gwarancji oraz datę odbioru robót przed upływem okresu rękojmi. Zamawiający powiadomi o tych terminach Wykonawcę w formie pisemnej. Przy odbiorach tych stosowane będą zasady, jak dla odbioru końcowego.

Organizacja placu budowy i prowadzenia robót

Wymagania stawiane Wykonawcy:

a) Teren budowy zostanie przekazany na 3 dni przed rozpoczęciem robót budowlanych. W czasie wykonywania robót Wykonawca zorganizuje miejsce budowy własnym staraniem i na własny koszt. Zaplecze budowy własne Wykonawcy.

b) Wykonawca zobowiązuje się do pokrywania kosztów związanych ze zużyciem mediów, tj. energii elektrycznej, energii cieplnej, wody oraz odprowadzania nieczystości ciekłych.

c) Wykonawca jest odpowiedzialny za jakość prac i ich zgodność z dokumentacją techniczną i specyfikacją techniczną wykonania i odbioru robót budowlanych oraz informacjami zawartymi w SIWZ.

d) Teren budowy należy wygrodzić i oznakować zgodnie z obowiązującymi przepisami. Należy wydzielić, oznakować i zabezpieczyć alternatywne ciągi pieszo – jezdne. Wygrodzenie terenu prowadzonych prac wyburzeniowych i remontowych powinno być szczelne. Zamknięcie ścianką tymczasową g-k z naciągniętą folią przeciw przenikaniu kurzu itp. Wykonawca robót jest odpowiedzialny za utrzymanie czystości zarówno na terenie budowy jak i w jego rejonie oraz na ciągach komunikacji ogólnodostępnej jeżeli będzie prowadził nimi obsługę budowy. Jeżeli dojedzie do jakiegokolwiek zabrudzenia czy zanieczyszczenia wykonawca jest zobowiązany natychmiast je usunąć na swój koszt.

e) Roboty budowlane nie mogą zakłócać funkcjonowania pracy Oddziałów Szpitala oraz innych jednostek Szpitala. Wykonawca ponosi odpowiedzialność finansową za wszelkie szkody wyrządzone Zamawiającemu lub osobom trzecim podczas prowadzenia prac budowlanych.

f) Od Wykonawcy wymagać się będzie:

- Przestrzegania zasad określonych w Procedurze zintegrowanego systemu zarządzania QP-034/0 – obowiązującej w Szpitalu.

- Przestrzegania zasad BHP i Sanitarno - Epidemiologicznych w czasie wykonywania robót.

- Wykonawca zobowiązany jest do posiadania odpowiedniego ubioru identyfikującego wykonawcę lub posiadania identyfikatora.

- Wykonawca będzie stosował się do wszystkich przepisów prawnych obowiązujących w zakresie bezpieczeństwa przeciwpożarowego i będzie odpowiedzialny za wszystkie straty powstałe w wyniku pożaru, który mógłby powstać w okresie realizacji robót lub został spowodowany przez któregokolwiek z jego pracowników.

- Opracowany przez Wykonawcę projekt organizacji robót musi być dostosowany do charakteru i zakresu przewidywanych robót. Ma on zapewnić zaplanowany sposób realizacji robót, w oparciu o zasoby techniczne, ludzkie i organizacyjne, które zapewnią realizację robót zgodnie z dokumentacją projektową.

- Powstałe w skutek z prowadzonymi robotami budowlanymi materiały podlegające recyklingowi Wykonawca przekaże Zamawiającemu. Pozostałe uzyskane z rozbiórki materiały Wykonawca zagospodaruje we własnym zakresie i na własny koszt.

- Wykonawca dostarczy odpowiednią ilość kontenerów do gromadzenia odpadów i zapewni ich regularny wywóz.

- Wykonawca zobowiązany jest do przestrzegania przepisów p. poż. . Teren budowy powinien wyposażyć w sprzęt ochrony pożarowej np. gaśnice. Pokrycie wszelkich ewentualnych strat poniesionych wskutek pożaru leży po stronie Wykonawcy.

- Podczas realizacji robót Wykonawca będzie przestrzegać przepisów BHP. W szczególności Wykonawca ma obowiązek zadbać, o odzież roboczą i środki ochrony osobistej swoich pracowników jak również o zaplecze socjalno- higieniczne. Sprzęt i urządzenia budowlane muszą być sprawne technicznie i nie mogą stanowić zagrożenia dla obsługujących je osób.

3.1.9. Parametry minimalne dla szafy RACK

Dostawa i instalacja szaf min. 42U do nowej serwerowni.

Szafy o wymiarach 800 x 1000, wysokość min. 42U i nośność min. 1000 kg,

Spełniające poniższe parametry:

.• Szafy o głębokości 1000mm trzy pary belek nośnych z płynną regulacją.

- Szafy muszą być dostępne według poniższej konfiguracji:

  - Drzwi przednie

    - szklane z bokami metalowymi i zamkiem z klamką

    - jednoskrzydłowe z perforacją o prześwicie 80%,z zamkiem z klamką

    - bez drzwi przednich

  - Drzwi tylne

    - blaszane, dwuskrzydłowe z perforacją o prześwicie 80%,z zamkiem z klamką

    - blaszane pełne, skrócone z zamkami jednopunktowymi bez klamki + jedna maskownica 3 U z przepustem szczotkowym zamontowana pod drzwiami

    - bez drzwi tylnych

  - Osłony boczne

    - blaszane pełne z zamkami jednopunktowymi

    - bez osłon bocznych

- Szafy o szerokości 800mm muszą umożliwiać zamontowanie pionowych prowadnic kabli w postaci:

  - maskownice metalowe z przepustami, z możliwością montażu minimum 10-ciu uchwytów kablowych. Uchwyty muszą mieć możliwość montażu w pionie i w poziomie

  - prowadnice grzebieniowe

- metalowa osłona z minimum 8-mioma dużymi przepustami kablowymi

- dwa rzędy elastycznych plastikowych grzebieni montowanych beznarzędziowo do osłony

- dwudzielna pokrywa montowana do grzebieni beznarzędziowo z możliwością otwierania na prawą lub lewą stronę

- Szafy mają być dostępne jako zmontowane, gotowe do wstawienia lub do samodzielnego montażu (płaska paczka łatwa do transportu i wstawienia przez wąskie drzwi).
- Pokryte lakierem proszkowym w ciemnym kolorze
- Możliwość zainstalowania wentylatora sufitowego z termostatem lub bez, zapewniającego wymianę powietrza w szafie oraz efektywne chłodzenie zainstalowanego tam sprzętu aktywnego.
- Możliwość zainstalowania filtracyjnej zaślepki podłogowej chroniącej przed zasysaniem kurzu do wnętrza szafy.
- Możliwość łączenia w zespoły kilku szaf.
- Możliwość zastosowania cokołu umożliwiającego wprowadzenie kabli z dowolnej strony.
- Konstrukcja w postaci lekkiego szkieletu stalowego zapewniającego dużą wytrzymałość mechaniczną oraz niezbędną sztywność.
- Uniwersalna konstrukcja drzwi przednich powinna zapewniać możliwość otwierania na prawą lub lewą stronę.
- Drzwi otwierane na szerokość 270 stopni
- Demontowalne osłony boczne oraz osłona tylna, zapewniające wygodny dostęp do wnętrza szafy z dowolnej strony.
- 19" rama montażowa z możliwością praktycznie płynnej regulacji głębokości położenia zapewniająca łatwość montażu dowolnego sprzętu.
- Regulowane stopki umożliwiające łatwe wypoziomowanie szafy nawet przy znacznych nierównościach podłogi.
- Pełne uziemienie wszystkich sekcji szafy bez konieczności osobnego zamawiania jakichkolwiek elementów uzupełniających.
- Szczotkowy przepust kablowy o dużej pojemności minimalizujący przedostawanie się kurzu do wnętrza szafy. Szafa powinna posiadać możliwość wprowadzania kabli przez ścianę tylną (przepust na dole nad podłogą i na górze pod sufitem) oraz przez podłogę. Przepust szczotkowy montowany jest w wybranym miejscu, a pozostałe otwory zaślepiane są metalową zaślepką.

Szafy należy wyposażyć w elementy organizujące kable krosowe:

- Wieszaki kablowe w ilości minimum jeden na 48 portów paneli krosowych

- Organizatory patchcordów światłowodowych zamykane i z tylnym przepustem

3.1.9.1. Panele krosujące miedziane

1. Kable należy zakończyć na 24 – portowym modularnym panelu krosowym o wysokości montażowej 1U posiadającym moduły RJ45 kat. min. 6A montowane indywidualnie w płycie czołowej panela, co zapewnia zwartą konstrukcję, łatwy montaż, terminowanie kabli oraz uniwersalne rozszycie kabla w sekwencji T568A lub T568B.
2. Panele proste lub kątowe.
3. Panel ma zawierać tylną prowadnicę kabla.
4. Panel ma zawierać zacisk uziemiający.
5. Kable instalacyjne, zakańczane na panelu, należy – w celu zapewnienia optymalnego prowadzenia – wesprzeć na prowadnicy kabli, montując je za pomocą opasek kablowych (należy zwrócić uwagę, aby zbyt mocno nie zaciskać opasek, mają one tylko lekko utrzymać kabel na prowadnicy).
6. Panele krosujące – krosownice należy umieszczać w każdym PD, miejscach wskazanych w tabelach i w serwerowniach.

3.1.9.2. Panele krosujące światłowodowe

1. Uniwersalny panel krosowy w stelażu powinien posiadać wysuwaną, metalową i blokowaną szufladę, w celu umożliwienia łatwego dostępu przy montażu modułów zatrzaskowych i ewentualnej rekonfiguracji połączeń w komfortowej odległości od szafy kablowej.
2. Mechanizm zamykania szuflady ma być zatrzaskowy, niepowodujący konieczności posiadania żadnych narzędzi do otwarcia panela i wysunięcia szuflady montażowej.
3. Panel standardowo ma być wyposażony w elementy zapasu włókna (prowadnice – krzyżaki), dławiki do wprowadzania i utrzymania kabli.

3.1.9.3. Kable miedziane

Kabel musi spełniać wymagania: **kategorii 6A** w paśmie do 500MHz.

Kabel powinien być ekranowany i posiadać konstrukcję **S/FTP**. Każda para powinna posiadać indywidualny ekran wykonany z folii aluminiowej jednostronnie lakierowanej. Dodatkowo kabel powinien posiadać wspólny ekran dla wszystkich par wykonany oplotem z drutu miedzianego ocynowanego.

Powłoka kabla powinna być w wykonaniu **LSZH** i w kolorze innym niż biały, szary i czerwony w celu odróżnienia kabli logicznych okablowania strukturalnego od kabli innych instalacji teletechnicznych.

Klasyfikacja odporności ogniowej**: B2ca-s1a,d1,a1.**

Kabel należy dostarczać na szpulach w odcinkach minimum 500m. Kabel konfekcjonowany na szpulach jest w dużo mniejszym stopniu podatny na uszkodzenia podczas instalacji oraz pozwala na bardziej efektywne wykorzystanie kabla przy krótkich odcinkach roboczych.

Standardy branżowe

ISO/IEC 11801 edycja 2:2010

TIA/EIA-568-C.2 Kategoria 6A

IEC 61156-5

Klasyfikacja odporności ogniowej

Regulacja Unii Europejskiej rr. 305/2011 (CPR)

EN 50575:2014+A:2016

Klasa B2ca-s1a,d1,a1

Parametry mechaniczne

Średnica przewodnika: 0.560 +/- 0.005mm

Materiał przewodnika: drut miedziany

Liczba par: 4

Średnica zew: 7.8 +/-0.5m

Ekran: Aluminium/Mylar

Oplot ekranujący: cynowana miedź

Minimalny promień gięcia instalacja: 8 x śred.zewn.

Maks. siła naciągu: 100N

Powłoka: LS0H

Kolor powłoki: fiolet RAL 4005

Waga 500m szpula: 29.4kg

Tolerancja dł. kabla: +/- 5%

Parametry elektryczne

Impedancja charakterystyczna Ohm:

1-250MHz 100 +/- 15 Ohm

250 -500 MHz 100 +/- 22 Ohm

Rezystancja Ohm/100m max: 9.38

Niezrównoważenie rezystancji % max: 5.0

Nierówność pojemności pf/100m max: 330

Rezystancja pętli Ohm/100m: 19.0

Napięcie znamionowe (Vdc): <80V

NVP 74%

Delay skew 1-500MHz ns/100m max: £45

Zgodność z PoE

Parametry transmisyjne

Częstotliwość MHz	RL ≥dB	ATT ≤dB	NEXT ≥dB	PHASE DELAY ≤ns	PSNEXT ≥dB	PSELFEXT ≥dB
1	20.0	-	74.3	570.00	72.3	64.8
4	23.0	3.8	65.3	552.00	63.3	52.8
8	24.5	5.3	60.8	546.70	58.8	46.7
10	25.0	5.9	59.3	545.40	57.3	44.8
16	25.0	7.5	56.2	543.00	54.2	40.7
20	25.0	8.4	54.8	542.10	52.8	38.8
25	24.3	9.4	53.3	541.20	51.3	36.8
31.25	23.6	10.5	51.9	540.40	49.9	34.7
62.5	21.5	15.0	47.4	538.60	45.4	28.9
100	20.1	19.1	44.3	537.50	42.3	24.8
200	18.0	27.6	39.8	536.60	37.8	18.8
250	17.3	31.1	38.3	536.30	36.3	16.8
300	16.8	34.3	37.1	536.10	35.1	15.3
500	15.2	45.3	33.8	535.60	31.8	10.8

3.1.9.4. Okablowanie światłowodowe

Należy zastosować uniwersalne kable światłowodowe **OS2** o konstrukcji **luźnej tuby**, która ma umożliwiać instalowanie wewnątrz jak i na zewnątrz pomieszczeń, włącznie z bezpośrednim układaniem w gruncie (w otoczeniu piasku). Kabel musi posiadać zabezpieczenie przed gryzoniami w postaci karbowanej **stalowej taśmy** oraz dodatkowe włókna szklane, jako element wzmacniający. Powłoka ma być wykonana w technologii **LS0H** która jest odporna na promieniowanie **UV** oraz ma być zgodna z Europejską Klasą **B2ca-s1a,d1,a1**.

Kabel powinien być dostępny z następującą ilością włókien: 4, 6, 8, 12 i 24. W niniejszym projekcie należy użyć kabla **12-to włóknowego**. Włókna powinny być ułożone w centralnej tubie wypełnionej żelem.

Standardy branżowe

Włókna:
IEC 60793-2-50 Kategoria B.1.3
ISO/IEC 11801:2002, Kategoria OS2 oraz OS1
ISO/IEC 24702: 2006, Kategoria OS2 oraz OS1
Rekomendacja ITU G.652.D and C, B, A
IEEE 802.3 – 2012
EN 50173-1:2007, Kategoria OS2 oraz OS1
Kabel:
ISO 11801-1,
EN 187 000,
IEC 60794-2,
EN 50173,
IEC 60794-2-20
Zgodność z dyrektywą ROSH
Testy palności:
Regulacja EU 305/2011 (CPR)
EN 50575:2014+A:2016
Europejska Klasa: B2ca-s1a,d1,a1

Parametry transmisyjne

Tłumienie kabla zgodne ze standardem IEC 60793-1-40:
1310 nm – 1625 nm: ≤ 0,3 dB/km
1550 nm: ≤ 0,25 dB/km
Współczynnik załamania fali optycznej zgodny ze standardem IEC 60793-1-22:
Dla fali 1310 nm: 1,467
Dla fali 1550 nm: 1,468
Dla fali 1625 nm: 1,468

Konstrukcja

Luźna tuba wypełniona żelem

Zbrojenie: pofalowana taśma stalowa 0,15 mm
Element wzmacniajacy: włókna szklane
Powłoka zewnętrzna: LS0H, stabilna względem promieni UV
Kolor powłoki: Żółty RAL 1018

Właściwości fizyczne wg IEC 60794-1-21/22

Średnica nominalna (mm)	-	2-24 włókna: 8,5 mm
Waga nominalna (Kg/km)	-	2-24 włókna: 100 kg/km
Maksymalne obciążenie instalacyjne (N)	E1	1500 N
Maksymalne obciążenie krótkotrwałe (N)	E1	750 N
Dopuszczalne zgniatanie (N/100mm)	E3	2000 N/100 mm
Dopuszczalne skręcanie	E7	5 cykli ± 1 skręt
Dopuszczalny promień zgięcia	E11	R = 85 mm
Zakresy temperatur	F1	Składowanie: od 40 °C do +70 °C Praca: od -40 °C do +70 °C Maksymalna zmiana tłumienia podczas pracy to: dla MM 0,5 dB/km dla SM 0,2 dB/km

3.1.10. Wykonanie połączenia światłowodowego z obecną serwerownią

Należy wykonać połączenie światłowodowe pomiędzy nową i obecną serwerownią wraz z rozszyciem na panelu.

3.1.10.1. Nowe gniazda i moduły

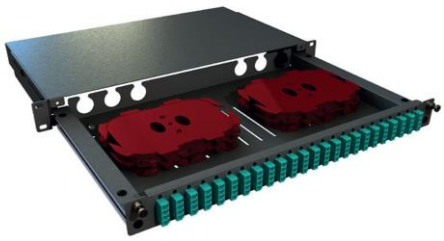
1. W płyty czołowe kątowe należy zamontować dwa ekranowane moduły gniazda RJ45 kat. min. 6A na zasadach KeyStone (w obiektach są zainstalowane moduły firmy Legrand kat 5).
2. Moduł gniazda RJ45 ma posiadać pełne ekranowanie z ekranem i uchwytem ekranu 360o kabla ekranowanego na całym obwodzie kabla.
3. Konstrukcja modułu ma podczas montażu składać się w szczelną całość, tworząc zintegrowaną i szczelną klatkę Faradaya, zabezpieczoną konstrukcyjnie nawet przed zakłóceniami pochodzącymi od modułów gniazd zainstalowanych w jednym rzędzie.
4. Konstrukcja modułu i uchwytu ekranu nie może zniekształcać konstrukcji kabla, ma również zapewniać maksymalną łatwość instalacji oraz gwarantować najwyższe parametry transmisyjne.
5. Wymaga się, aby każdy moduł gniazda RJ45 posiadał możliwość uniwersalnego terminowania kabli, tj. w sekwencji T568A lub T568B.
6. Każdy moduł ma być zarabiany narzędziami dedykowanymi, uniwersalnymi lub też beznarzędziowo.
7. Moduły ekranowane gniazd RJ45, mają umożliwiać terminację drutu miedzianego o średnicy od 0,51 do 0,65mm (24 – 22 AWG).
8. Moduł Keystone RJ45 - ekranowany, kat. min. 6A.
9. Styk ekranu – Stal nierdzewna.
10. Schemat T568A & T568B nadrukowany na pokrywie IDC.
11. Ilość cykli połączeniowych - Minimum 750 cykli.

12. Średnica przewodnika – drut 24-22 AWG.
13. Aby potwierdzić utrzymanie parametrów elektrycznych gniazd podczas długotrwałego użytkowania łącznie z PoE+ producent powinien przedstawić raport z testów wg normy IEC 60512-99-001 Connectors used in twisted pair communication cabling with remote power.

3.1.10.2. Panele krosujące światłowodowe

Panele światłowodowe powinny spełniać poniższe wymagania:

1. Trwała, sztywna konstrukcja wykonana z blachy stalowej pokrytej powłoką antykorozyjną (lakier proszkowy). Nie dopuszcza się paneli z tworzyw sztucznych.
2. Wysokość panela 1U.
3. Panel powinien składać się korpusu panela tj. obudowy montowanej w ramie 19” oraz wymiennych paneli przednich (płyt czołowych) wpinanych w korpus panela.
4. Producent okablowania strukturalnego powinien posiadać w swojej ofercie płyty czołowe dla:
    a. adapterów ST, SC, LC, FC, SC/APC, LC/APC
    b. Kaset plug&play ze złączami MPO/MTP
5. Płyty czołowe powinny mieć wysokość korpusu czyli 1U oraz umożliwiać skalowanie ilości zakańczanych włókien od dwóch do minimum 96-ciu poprzez wpinanie odpowiedniej ilości adapterów.
6. Musi istnieć możliwość wymiany panela przedniego (płyty czołowej) na inny (np. o większej pojemności) bez konieczności deinstalacji zainstalowanych kabli i ponownego terminowania złącz światłowodowych. (W takiej sytuacji wystarczy wypiąć złącza z adapterów, wymienić panel przedni na odpowiedni oraz wpiąć złącza. Nowo dołożone kable oczywiście muszą zostać wprowadzone do panela i zarobione złączami.)
7. Panel powinien posiadać konstrukcję wysuwaną, tj. pozwalająca na wysunięcie płyty czołowej oraz ustawienie pod kątem umożliwiając łatwy dostęp do zapasu włókna, złącz światłowodowych i kasety spawów. Szuflada powinna posiadać blokadę zabezpieczającą przed niepożądanym wysunięciem np. w momencie wypinania kabla krosowego.
8. Adaptery światłowodowe powinny być mocowane do płyt czołowych za pomocą śrub, zapewni to trwałe połączenie oraz stabilność połączeń światłowodowych.
9. Panel powinien posiadać w komplecie odpowiednie akcesoria umożliwiające organizowanie zapasu włókien światłowodowych, trwałe mocowanie kabli przychodzących (odpowiednio nacięta śruba z nakrętką służąca do mocowania włókna szklanego bądź kevlaru wzmacniającego kabel), przepusty kablowe chroniące powłokę kabla przed uszkodzeniem. Powinien posiadać również odpowiednie zaczepy pozwalające na montaż kaset spawów (minimum 96 spawów w jednym panelu).
10. Panel musi być wyposażony w czytelny system oznaczania kanałów.



Panel światłowodowy ma mieć wysokość **4U** i konstrukcję konfigurowalnej obudowy do przechowywania i zakańczania przychodzących kabli światłowodowych, zamontowanej w ramie

19’’. Obudowę można konfigurować, dobierając kasety MPO, płytki z adapterami oraz uniwersalne kasety światłowodowe wyposażone w adaptery, pigtaile i tace spawów. Panel ma posiadać **24 sloty** do montażu w/w płytek lub kaset zapewniając możliwość zakończenia **576-ciu włókien** na złączach LC. Konstrukcja obudowy ma uwzględniać potrzeby instalatora związane z początkowym montażem oraz użytkownika końcowego związane z dostępem, konserwacją i ochroną światłowodów.
Panel ma zawierać mocne prowadnice z łożyskami kulkowymi do płynnego i ograniczonego wysuwania szuflady. Umożliwia to dostęp do kabli krosowych, a jednocześnie ochronę zainstalowanych kabli krosowych i pionowych przed uszkodzeniem podczas ponownego wsuwania panela.
Panel ma posiadać lekki, zdejmowany, aluminiowy panel wierzchni/tylny umożliwiający łatwy dostęp do tylnej lub górnej części obudowy bez potrzeby używania narzędzi.
Zainstalowane kasety lub płytki mają być cofnięte do środka i schowane za zamykanymi, stalowymi drzwiczkami przednimi
Każdy punkt wejścia kabla ma mieć miejsca do zamocowania miedzianego bolca uziemienia
Panel ma mieć możliwość zainstalowania w szafie bez naruszania sprzętu zainstalowanego powyżej i poniżej

Parametry mechaniczne:
Materiał Podstawa i szuflada: Stal o grubości 1,52 mm walcowana na zimno
Góra: Aluminium 1,52 mm
Powłoka: Czarny lakier proszkowy
Szpulki kablowe: Termoplastyczne tworzywo UL94V-O
Wymiary Szerokość: 483 mm Wysokość: 176 mm Głębokość: 470 mm
Waga panela: 8,3 kg

Elementy składowe Panela Światłowodowego:
Skrzynka światłowodowa (zmontowana fabrycznie) zawierająca:
– Szufladę światłowodową z arkuszem etykiet do portów
– Regulowany/wielopozycyjny miedziany bolec do uziemienia/zacisk do elementu podtrzymującego kabel światłowodowy
– 4 paski rzepowe (1,9 cm x 20,32 cm – 3⁄4” x 8”)
– 2 szpulki do porządkowania kabli
– 4 pętle do porządkowania kabli krosowych
– Etykietę ostrzegawczą n
Sprzęt do montażu w ramie 19”
Instrukcja montażu

Panel należy wyposażyć w płytę czołową umożliwiającą terminowanie różnych mediów (miedziane i światłowodowe) oraz montaż następujących typów złączy (adapterów):

11. Światłowodowe: ST, SC, SC/APC, FC, LC, LC/APC
12. Miedziane: RJ45, BNC, RCA, F Video, S Video

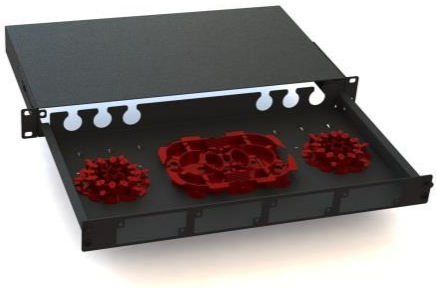
Dodatkowo ta sama płyta czołowa musi mieć możliwość montażu kaset światłowodowych z wejściem MPO.

Kabel 24-ro włóknowy należy zakończyć w jednej **kasecie** wyposażonej w adaptery **6 x LC Quad OS2 „Low Loss".** Kasetę należy umieścić w płycie czołowej o wysokości 1U. Płyta czołowa musi umożliwiać montaż minimum 4-ech takich kaset. Niewykorzystane pola należy zaślepić i pozostawić jako rezerwę.
Włókna należy zakończyć metodą dospawania pig-taili. Wszystkie spawy i pig-taile kabla należy zamknąć w jednej obudowie (kasecie), tak aby podczas montażu dodatkowych kabli i/lub mediów w panelu nie narażać istniejących połączeń na uszkodzenie.

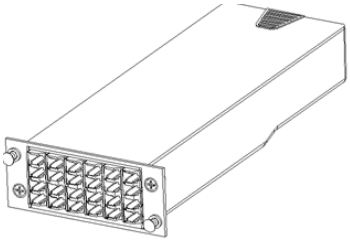
Cechy kaset:

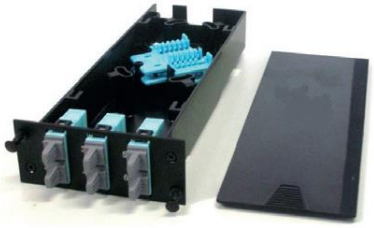
- Duża gęstość – maksymalnie 24 włókna w kasecie
- Kasety muszą zapewniać zarządzanie zapasem włókna oraz mocowanie dla spawów światłowodowych
- Musi być zapewniony odpowiedni promień gięcia włókna
- Kasety muszą być dostępne w postaci kompletnych zestawów (z adapterami, pig-tailami oraz tacami spawów) jak również w postaci oddzielnych komponentów do samodzielnej konfiguracji

Standardy branżowe
TIA/EIA 568-B.3:2000, ISO 11801:2002,
EN50173:2007
Parametry mechaniczne
Wymiary kasety:
długość [mm]: 185
szerokość [mm]: 63
wysokość[mm]: 33
Materiał obudowy: tworzywo sztuczne ABS
Materiał pokrywy: tworzywo sztuczne ABS

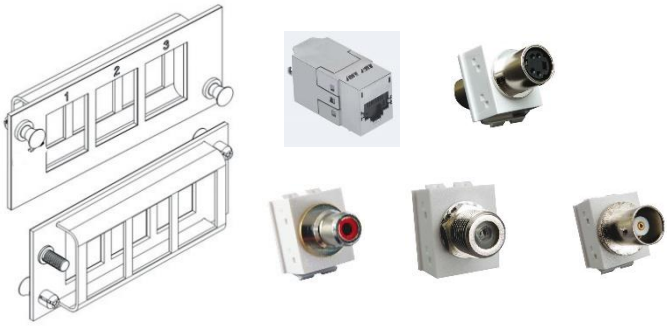


Korpus panela światłowodowego z płytą czołową





Kasety światłowodowe



Adapter i złącza dla mediów miedzianych

Panel należy wyposażyć w płytę czołową 1U umożliwiającą terminowanie różnych mediów (miedziane i światłowodowe) oraz montaż następujących typów złączy (adapterów):

13. Światłowodowe: ST, SC, SC/APC, FC, LC, LC/APC
14. Miedziane: RJ45, BNC, RCA, F Video, S Video

Dodatkowo ta sama płyta czołowa musi mieć możliwość montażu kaset światłowodowych z wejściem MPO. Płyta czołowa musi umożliwiać montaż minimum 4-ech takich kaset. Niewykorzystane pola należy zaślepić i pozostawić jako rezerwę.

Kable światłowodowe należy zakończyć na wielofunkcyjnych panelach spełniających poniższe wymagania:

- Trwała, sztywna konstrukcja wykonana z blachy stalowej pokrytej powłoką antykorozyjną (lakier proszkowy). Nie dopuszcza się paneli z tworzyw sztucznych.
- Wysokość panela 1U.
- Panel powinien składać się korpusu panela tj. obudowy montowanej w ramie 19” oraz wymiennych paneli przednich (płyt czołowych) wpinanych w korpus panela.
- Producent okablowania strukturalnego powinien posiadać w swojej ofercie płyty czołowe dla:
    - adapterów ST, SC, LC, FC, SC/APC, LC/APC
    - Kaset plug&play ze złączami MPO/MTP
- Płyty czołowe powinny mieć wysokość korpusu czyli 1U oraz umożliwiać skalowanie ilości zakańczanych włókien od dwóch do minimum 96-ciu poprzez wpinanie odpowiedniej ilości adapterów.
- Musi istnieć możliwość wymiany panela przedniego (płyty czołowej) na inny (np. o większej pojemności) bez konieczności deinstalacji zainstalowanych kabli i ponownego terminowania złącz światłowodowych. (W takiej sytuacji wystarczy wypiąć złącza z adapterów, wymienić panel przedni na odpowiedni oraz wpiąć złącza. Nowo dołożone kable oczywiście muszą zostać wprowadzone do panela i zarobione złączami.)
- Panel powinien posiadać konstrukcję wysuwaną, tj. pozwalająca na wysunięcie płyty czołowej oraz ustawienie pod kątem umożliwiając łatwy dostęp do zapasu włókna, złącz światłowodowych i kasety spawów. Szuflada powinna posiadać blokadę zabezpieczającą przed niepożądanym wysunięciem np. w momencie wypinania kabla krosowego.

- Adaptery światłowodowe powinny być mocowane do płyt czołowych za pomocą śrub, zapewni to trwałe połączenie oraz stabilność połączeń światłowodowych.
- Panel powinien posiadać w komplecie odpowiednie akcesoria umożliwiające organizowanie zapasu włókien światłowodowych, trwałe mocowanie kabli przychodzących (odpowiednio nacięta śruba z nakrętką służąca do mocowania włókna szklanego bądź kevlaru wzmacniającego kabel), przepusty kablowe chroniące powłokę kabla przed uszkodzeniem. Powinien posiadać również odpowiednie zaczepy pozwalające na montaż kaset spawów (minimum 96 spawów w jednym panelu).
- Panel musi być wyposażony w czytelny system oznaczania kanałów.

Panel należy wyposażyć w **płytę czołową** umożliwiającą terminowanie różnych mediów (miedziane i światłowodowe) oraz montaż następujących typów złączy (adapterów):

- Światłowodowe: ST, SC, SC/APC, FC, LC, LC/APC
- Miedziane: RJ45, BNC, RCA, F Video, S Video

Dodatkowo ta sama płyta czołowa musi mieć możliwość montażu kaset światłowodowych z wejściem MPO.

Kabel 12-to włóknowy należy zakończyć w jednej **kasecie** wyposażonej w adaptery **12 x LC OS2 „Low Loss”.** Kasetę należy umieścić w płycie czołowej o wysokości 1U. Płyta czołowa musi umożliwiać montaż minimum 4-ech takich kaset. Niewykorzystane pola należy zaślepić i pozostawić jako rezerwę.
Włókna należy zakończyć metodą dospawania pig-taili. Wszystkie spawy i pig-taile kabla należy zamknąć w jednej obudowie (kasecie), tak aby podczas montażu dodatkowych kabli i/lub mediów w panelu nie narażać istniejących połączeń na uszkodzenie.

Cechy kaset:
- Duża gęstość – maksymalnie 24 włókna w kasecie
- Kasety muszą zapewniać zarządzanie zapasem włókna oraz mocowanie dla spawów światłowodowych
- Musi być zapewniony odpowiedni promień gięcia włókna
- Kasety muszą być dostępne w postaci kompletnych zestawów (z adapterami, pig-tailami oraz tacami spawów) jak również w postaci oddzielnych komponentów do samodzielnej konfiguracji

Standardy branżowe
TIA/EIA 568-B.3:2000, ISO 11801:2002,
EN50173:2007
Parametry mechaniczne
Wymiary kasety:
długość [mm]: 185
szerokość [mm]: 63
wysokość[mm]: 33
Materiał obudowy: tworzywo sztuczne ABS
Materiał pokrywy: tworzywo sztuczne ABS

3.1.11. Wykonanie połączeń światłowodowych z PD

Należy wykonać połączenia światłowodowe pomiędzy nową serwerownią a wszystkie PD w szpitalu za pomocą światłowodów SM minimum 12j z rozszyciem na panelach ze złączem LC/PC.

PD Nazwa	Orientacyjna odległość do Serwerowni w Dziale Techn. [m]
D0_Poradnie	360
D1_ChemDz	400
D2_Informatycy	400
B0_Analityka	280
B1_RTG	300
B1_Onkologia	280
B2_USG	300
E2_BlokOp	250
E1_Anestezjologia	250
A0_Angiokardiografia	230
A0_Rezonans	210
A0_Endoskopia	200
A1_Rehabilitacja	200
A2_Ortopedia	200
A3_ChirOg	210
A4_Wewn2	215
A5_Kardiologia	220
A5_Informatycy	260
A6_Urologia	225
A7_Okulistyka	230
C1_SOR	270
C1_SOR_URAZ	270
C2_BlokPor	300
Hpiwnica_Magazyn	240
H0_Neurologia	250
H1_Pediatria	300
H2_Otolaryngologia	260
H3_ChirDz	300
H2_Noworodki	330
Radioterapia	160
Radioterapia_serwerownia	160
Kuchnia	100
Pralnia	150

Patomorfologia	130
CentralaTel	100
DziałTechniczny	30
Psych_parter	420
Psych_1	430
Psych_2	440
Uzaleznienia_1	700
Uzaleznienia_2	750
Uzaleznienia_3	750
Hotel	650
BOP	420

3.1.11.1. Nowe gniazda i moduły

1. W płyty czołowe kątowe należy zamontować dwa ekranowane moduły gniazda RJ45 kat. min. 6A na zasadach KeyStone (w obiektach są zainstalowane moduły firmy Legrand kat 5).
2. Moduł gniazda RJ45 ma posiadać pełne ekranowanie z ekranem i uchwytem ekranu 360o kabla ekranowanego na całym obwodzie kabla.
3. Konstrukcja modułu ma podczas montażu składać się w szczelną całość, tworząc zintegrowaną i szczelną klatkę Faradaya, zabezpieczoną konstrukcyjnie nawet przed zakłóceniami pochodzącymi od modułów gniazd zainstalowanych w jednym rzędzie.
4. Konstrukcja modułu i uchwytu ekranu nie może zniekształcać konstrukcji kabla, ma również zapewniać maksymalną łatwość instalacji oraz gwarantować najwyższe parametry transmisyjne.
5. Wymaga się, aby każdy moduł gniazda RJ45 posiadał możliwość uniwersalnego terminowania kabli, tj. w sekwencji T568A lub T568B.
6. Każdy moduł ma być zarabiany narzędziami dedykowanymi, uniwersalnymi lub też beznarzędziowo.
7. Moduły ekranowane gniazd RJ45, mają umożliwiać terminację drutu miedzianego o średnicy od 0,51 do 0,65mm (24 – 22 AWG).
8. Moduł Keystone RJ45 - ekranowany, kat. min. 6A.
9. Styk ekranu – Stal nierdzewna.
10. Schemat T568A & T568B nadrukowany na pokrywie IDC.
11. Ilość cykli połączeniowych - Minimum 750 cykli.
12. Średnica przewodnika – drut 24-22 AWG.
13. Aby potwierdzić utrzymanie parametrów elektrycznych gniazd podczas długotrwałego użytkowania łącznie z PoE+ producent powinien przedstawić raport z testów wg normy IEC 60512-99-001 Connectors used in twisted pair communication cabling with remote power.

3.1.12. Parametry minimalne dla Switch dostępowych

1.	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej
2.	Wymagane parametry fizyczne: a) możliwość montażu w stelażu/szafie 19” b) wysokość maksymalna 1U c) minimum jeden zasilacz 230V AC, moc zasilacza zapewniająca budżet mocy dla portów PoE minimum 380W. d) zakres temperatur pracy ciągłej co najmniej od 0 do +50 °C e) zakres wilgotności pracy co najmniej 5% - 90% f) port USB umożliwiający podłączenie zewnętrznej pamięci flash (gniazdo musi być dostępne od frontu urządzenia). g) ochrona przed przepięciami: ±4 kV h) waga urządzenia nie większa niż 6kg i)
3.	Przełącznik musi posiadać minimum: ● 48 portów 10/100/1000BASE-T PoE+ zgodnych z 802.3at oraz 802.3af ● 4 porty 10GE SFP+ Wszystkie porty muszą być dostępne od frontu urządzenia.
4.	Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności: a) Zarządzanie stosem poprzez jeden adres IP b) Do min. 9 jednostek w stosie c) Magistrala stackująca o wydajności minimum 40Gb/s d) Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation) e) Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree f) Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia. Zamawiający dopuszcza, aby możliwość łączenia w stosy była realizowana za pomocą portów typu uplink 10G SFP+.
5.	Układ przełączający o wydajności min. 176 Gbps, wydajność przełączania przynajmniej 132 Mpps
6.	Obsługa min. 32 000 adresów MAC
7.	Wbudowana pamięć RAM min. 512MB. Procesor minimum dwurdzeniowy
8.	Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 500 MB
9.	Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)

10.	Możliwość skonfigurowania min. 1000 interfejsów vlan interface SVI działających równocześnie
11.	Obsługa ramek jumbo o wielkości min. 9216 bajtów
12.	Obsługa standardów IEEE: a) CFM zgodny z 802.1ag b) EFM zgodny z 802.3ah
13.	Obsługa protokołu GVRP lub GARP
14.	Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu MSTP
15.	Obsługa min. 4 000 tras dla routingu IPv4
16.	Obsługa min. 1 000 tras dla routingu IPv6
17.	Obsługa protokołów routingu OSPF, OSPFv3, RIP, RIPng, PIM-SM, PIM-DM. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania
18.	Obsługa wirtualnych tablic routingu-forwardingu (VRF)
19.	Obsługa protokołów LLDP i LLDP-MED
20.	Przełącznik musi posiadać funkcjonalność DHCP Server
21.	Obsługa ruchu multicast: ● IGMP v1, v2 i v3 ● IGMP Snooping v1, v2 i v3 ●
22.	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci: a) min. 4 poziomy dostępu administracyjnego poprzez konsolę b) autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL c) możliwość utworzenia minimum 2000 list ACL d) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www e) zarządzanie urządzeniem przez HTTPS, SNMPv3 i SSHv2 za pomocą protokołów IPv4 i IPv6 f) możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP g) obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard h) możliwość synchronizacji czasu zgodnie z NTP i)
23.	Obsługa funkcjonalności UDLD lub równoważnej
24.	Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach: ● klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP

	• wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR
25.	Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA. Urządzenie musi umożliwiać konfigurację liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP w ramach pojedynczej próbki. Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania
26.	Wymagane opcje zarządzania: a) możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN b) plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC) c) urządzenie musi posiadać wbudowany port USB znajdujący się od strony portów, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych d) dedykowany port konsoli, musi się znajdować od strony portów i być zgodny ze standardem RS-232 e)
27.	Wraz z urządzeniami muszą zostać dostarczone: a) pełna dokumentacja w języku polskim lub angielskim b) dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana c)
28.	Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy
29.	Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski
30.	Zamawiający wymaga, aby przełącznik posiadał 3-letni serwis gwarancyjny, świadczony przez Wykonawcę na bazie wsparcia serwisowego producenta. Wymiana uszkodzonego elementu w trybie 9x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia
31.	Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres serwisu gwarancyjnego dla urządzeń

3.1.13. Parametry minimalne dla AP WiFi

1. Urządzenie do pracy w sieci bezprzewodowej.
2. Urządzenie musi posiadać oprogramowanie do pracy w trybie tzw „lekkiego AP” pod kontrolą kontrolera bezprzewodowego oraz możliwość pracy jako tzw “grubego AP (FAT AP)”.
3. Obsługa protokołu umożliwiającego oddzielenie ruchu lokalnego (wychodzącego bezpośrednio z AP) od ruchu kierowanego do kontrolera.
4. Obsługa VLAN.
5. Obsługiwane standardy radiowe:
    5.1. 802.11a/b/g/n/ac/ac Wave 2/11ax, jednoczesna obsługa minimum 16 SSID dla każdego radia
    5.2. moc interfejsów radiowych 25dBm dla 2,4GHz oraz 28dBm dla 5GHz z możliwością zmniejszenia poziomu
6. Wbudowane anteny działające w 2,4GHz i 5GHz. Wsparcie dla modulacji 1024QAM.
7. Ilość portów:
    7.1. Minimum 1 port RJ-45 auto-sensing 10/100/1000 port (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE802.3ab Type 1000Base-T) typu PoE IN (z możliwością zasilania poprzez technologię PoE+)
    7.2. Minimum 1 port RJ-45 auto-sensing 10/100/1000 port (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE802.3ab Type 1000Base-T)
    7.3. Port USB umożliwiający instalację modułu IoT
8. Urządzenie przeznaczone do zainstalowania wewnątrz budynków. Wraz z urządzeniem należy dostarczyć zestawy montażowe
9. Wbudowane anteny minimum 4dBi dla 2,4GHz oraz 5dBi dla 5GHz z pracą w standardzie minimum MIMO: 2.4G: 2x2, 5G: 4x4
10. Wsparcie dla standardów bezpieczeństwa: WPA, WPA2, WPA3, WPA2-PPSK, 802.1x, 802.11w, DHCP Snooping, Dynamic ARP Inspection (DAI) lub równoważny, IP Source Guard (IPSG) lub równoważny oraz tworzenie ACL
11. Wsparcie dla roamingu zgodnego z 802.11k, 802.11v, 802.11r
12. Obsługa minimum 1000 równocześnie podłączonych użytkowników do punktu dostępowego
13. Wydajność minimum 5Gbps w tym minimum 500Mbps dla 2.4GHz oraz 4.5Gbps dla 5GHz
14. Pamięć RAM minimum 1GB
15. Pamięć flash minimum 512MB
16. Parametry otoczenia
    16.1. temperatura pracy: -10º do +50ºC
    16.2. temperatura przechowywania: -40º do +70ºC
    16.3. wilgotność pracy: 5% - 90%
17. Możliwość podłączenia zewnętrznego zasilacza DC 12V
18. Obsługa zasilania zgodnego z 802.3at
19. Obsługa BLE w wersji 5.0

20. Zużycie energii: nie więcej niż 20W
21. Zarządzanie urządzeniem z wykorzystaniem kontrolera tego samego producenta oraz SSHv2, HTTPS, SNMPv3 w trybie niezależnym (FAT AP).
22. Kompatybilność dla protokołów oraz standardów sieciowych takich jak: IPv6, SAVI IPv6, 802.1q, 802.3ab, LLDP, MDI, MDI-X, mDNS, NAT, GRE
23. Obsługa NTP
24. Funkcjonalność szyfrowania komunikacji pomiędzy access-pointem a kontrolerem WLAN z wykorzystaniem standardów DTLC lub IPSec celem zapewnienia poufności w wymianie danych
25. Obsługa funkcjonalności pozwalającej na wymuszanie i priorytetyzowanie połączeń użytkowników dla radia 5 GHz
26. Certyfikaty dotyczące bezpieczeństwa: UL 60950-1, EN 60950-1
27. Waga urządzenia nie większa niż 1,5kg
28. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.
29. Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski
30. Bezpłatny dostęp do aktualizacji oprogramowania przez cały okres gwarancji serwisowej dla urządzeń
31. Zamawiający wymaga, aby wszystkie dostarczone punkty dostępowe posiadały 5-letni serwis gwarancyjny, świadczony przez Wykonawcę na bazie wsparcia serwisowego producenta. Wymiana uszkodzonego elementu w trybie 8x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia

3. 1.14 Parametry minimalne dla UTM

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. System bezpieczeństwa musi zostać dostarczony w postaci klastra wysokiej dostępności HA co najmniej active/passive.

Dla elementów systemu bezpieczeństwa wykonawca musi zapewnić wszystkie poniższe funkcjonalności:

1. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
2. System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/1000
3. System realizujący funkcję Firewall musi dysponować minimum 4 interfejsami optycznymi 10GbE (SFP+) oraz 2 interfejsami optycznymi 1GbE (SFP)

4. Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
5. W zakresie Firewall'a obsługa nie mniej niż 1 500 000 jednoczesnych połączeń oraz 75 000 nowych połączeń na sekundę.
6. System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 120 GB SSD do celów logowania i raportowania.
7. System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
8. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:
    a. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
    b. Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS). System AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.
    c. Poufność danych - IPSec VPN oraz SSL VPN
    d. Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
    e. Kontrola stron Internetowych – Web Filter [WF]
    f. Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3)
    g. Kontrola pasma oraz ruchu [QoS i Traffic shaping]
    h. Kontrola aplikacji oraz rozpoznawanie ruchu P2P
    i. Analiza ruchu szyfrowanego protokołem SSL
9. Wydajność systemu Firewall minimum 30 Gbps
10. Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus minimum 2,5 Gbps
11. Wydajność ochrony przed atakami (IPS) minimum 13 Gbps
12. Wydajność VPN IPSec, nie mniej niż 4 Gbps
13. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
    a. Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site
    b. Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem
    c. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
    d. Praca w topologii Hub and Spoke oraz Mesh
    e. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth
    f. Obsługa ssl vpn w trybach portal oraz tunel
14. Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP.
15. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
16. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).
17. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.

18. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
19. Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów. Dodatkowo musi być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
20. Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
21. Baza filtra WWW pogrupowana w min 50 kategorii tematycznych. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
22. Automatyczne ściąganie sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
23. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
    a. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
    b. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
    c. Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych
    d. Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny
24. W zakresie realizowanych funkcjonalności systemu raportowania i przeglądania logów, wymagane jest nie mniej niż:
    a. Posiadanie predefiniowanych raportów dla ruchu WWW, modułu IPS, skanera antywirusowego i antyspamowego
    b. Generowanie co najmniej 25 różnych typów raportów
25. System raportowania i przeglądania logów wbudowany w system bezpieczeństwa nie może wymagać dodatkowej licencji do swojego działania
26. Element oferowanego systemu bezpieczeństwa realizujący zadanie Firewall musi posiadać certyfikat ICSA lub EAL4+ dla rozwiązań kategorii Network Firewall.
27. Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
28. Wymaga się, aby dostawa obejmowała również:
    a. Minimum 36-miesięczną gwarancję producentów na dostarczone elementy systemu liczoną od dnia zakończenia wdrożenia całego systemu.
    b. Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres minimum 36 miesięcy liczoną od dnia zakończenia wdrożenia całego systemu.

29. Należy zapewnić bezpłatne certyfikowane szkolenia (6 x 8h) w zakresie użytkowania i administrowania wdrożonego urządzenia UTM. Szkolenie ma zostać przeprowadzone dla maksymalnie 8 osób i uwzględniać informacje z zakresu wdrożonego urządzenia (m.in. definiowanie polityki filtrowania (Firewall i NAT) oraz trasy routingu, kontrola dostępu do stron internetowych (http i https),

konfiguracja polityki bezpieczeństwa dla uwierzytelnionych użytkowników, konfiguracja różnego typy wirtualnych sieci prywatnych (VPN) - IPSec VPN i SSL VPN, zaawansowana konfiguracja z poziomu GUI, konfiguracja polityki silnika IPS, zarządzanie infrastrukturą klucza publicznego (PKI) i konfiguracja transparentnego uwierzytelniania, budowa tunelu IPSec VPN w oparciu o certyfikaty, konfiguracja i zarządzanie urządzeniami w ramach klastra HA itp.). Szkolenia muszą być zakończone egzaminem i certyfikatem potwierdzającym wspomniane umiejętności wydanym przez producenta systemu. Szkolenia mogą odbyć się w formie zdalnej.

3. 1.15 Parametry minimalne dla systemu bezpieczeństwa sieci i danych

3.1.15.1. Parametry minimalne dla serwera dla SIEM

Element konfiguracji	Wymagania minimalne
Obudowa	Obudowa rack o wysokości max 2U z możliwością instalacji min. 8 dysków 3,5 cala Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych z czujnikiem otwarcia obudowy współpracującym z BIOS oraz kartą zarządzającą.
Płyta główna	Płyta główna oznaczona trwale logiem producenta z możliwością zainstalowania dwóch procesorów.
Procesor	Zainstalowane dwa procesory min. 20-rdzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku Baseline SPECint_base2017 min. 238 punktów dostępnym na stronie www.spec.org dla oferowanego modelu serwera.
Pamięć operacyjna	Minimum 256 GB RDIMM DDR4 w modułach nie mniejszych niż 32GB. Zabezpieczenia pamięci: ECC, Memory Rank Sparing i/lub Lockstep.
Sloty rozszerzeń	Minimum 2 wolne sloty PCIE 3.0 po zamontowaniu kontrolera dysków oraz kart sieciowych.
Dysk twardy	Serwer musi posiadać zainstalowane min. 2 dyski SSD na system wirtualny o pojemności minimum 480GB każdy. Dyski SSD muszą zostać skonfigurowane min. w RAID 1. Zainstalowane minimum 20TB powierzchni dyskowej surowej na dyskach HDD
Kontroler	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 5, 10, 50, 6, 60 orazJBOD jednocześnie. Kontroler musi posiadać minimum 2GB pamięci cache.
Interfejsy sieciowe	Serwer musi posiadać zainstalowane: - min. dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT - min. cztery interfejsy sieciowe 10/25Gb typu SFP28
Karta graficzna	Zintegrowana karta graficzna
Porty	Minimum 4 porty USB 3.0 w tym min. 2 porty USB z tyłu, 1 port VGA z tyłu, opcjonalne (nie wymagane w chwili dostawy) rozwiązanie

	producenta z cyfrowym portem video na froncie obudowy, dedykowany port 1Gb Ethernet do zarządzania, port szeregowy
Dodatkowe napędy	Możliwość instalacji wewnętrznego napędu DVD-ROM lub DVD-RW (dopuszcza się rozwiązania zewnętrzne)
Zasilacz	Redundantne dwa zasilacze, Hot-Plug o mocy minimum 800W każdy, wersja minimum titanium
Chłodzenie	Redundantne wentylatory hot-swap
Wsparcie dla Systemów Operacyjnych i Systemów Wirtualizacyjnych	Microsoft Windows Server Canonical Ubuntu Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware Citrix XenServer ClearOS Zainstalowany system wirtualizacyjny
System operacyjny	Zainstalowany najnowszy system operacyjny klasy Windows Serwer lub równoważny (Linux) w ilości po 2 licencje na każdy serwer. Oprogramowanie wirtualizacyjne dla systemu SIEM.
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.
Gwarancja	Gwarancja realizowana w miejscu instalacji sprzętu (min. trzy lata) Możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta Wszystkie naprawy gwarancyjne powinny być realizowane na miejscu

3.1.15.2. Parametry minimalne dla systemu dyskowego dla SIEM

W kontekście prawnej konieczności zapewnienia niezmienności i trwałości danych przez okres powyżej 20 lat, w ramach przedmiotowego projektu należy zbudować centralne archiwum, w którym składowane będą zarówno dane EDM jak również wszelkie wyniki badań w tym dane obrazowe (PACS), a także inne dane wymagające długoletniej archiwizacji. Archiwum powinno być niezależne od pozostałych systemów.

Element konfiguracji	Wymagania minimalne
Architektura procesora	64 bit
Procesor liczba rdzeni	Nie mniej niż 6 o taktowaniu nie niższym niż 3,4 GHz
Pamięć RAM	Nie mniej niż 128 GB ECC DDR4
Pamieć RAM liczba slotów	Minimum 4 sloty

Pamięć Flash	Nie mniej niż 5GB
Liczba zatok na dyski twarde	Minimum 24, Zainstalowane w urządzeniu dyski o łącznej pojemności surowej minimum 300TB
Obsugiwane dyski twarde	3.5" SATA oraz 2.5" SATA / SSD SATA
Pojemność dysków twardych jakie można stosować	do 18 TB
Opcjonalna możliwość podłączenia modułu rozszerzającego	Tak, minimum 9
Porty LAN	Minimum 2 x 10 Gb/s RJ-45 oraz 2 x 10 Gb/s SFP+
Diody LED	HDD 1–24, stan urządzenia, LAN
Porty USB	min. 1 gniazdo typu C USB 3.2 Gen2 10 Gb/s min. 1 gniazdo typu A USB 3.2 Gen2 10 Gb/s
Przyciski	Reset, Zasilanie
Typ obudowy	RACK, max 4U
Dopuszczalna temperatura pracy	od 0 do 40˚C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Redundatne zasilacze
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: ZFS Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Łączenie usług z interfejsem	Tak
Szyfrowanie udziałów	Tak, min AES 256
Szyfrowanie dysków	Tak

zewnętrznych	
Zarządzanie dyskami	RAID 0,1,5,50,6,60,10, Triple Parity, Triple Mirror Konfiguracja priorytetu odbudowy grup RAID RAID HotSpare i Global HotSpare SSD Trim HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Wykrywanie uszkodzenia i automatyczna naprawa danych Cache odczytu z wykorzystaniem dysków SSD Cache odczytu i dziennik zapisu z wykorzystaniem dysków SSD Funkcjonalność migawek udziałów oraz LUN, wraz z możliwością ich replikacji na drugie urządzenie
Wbudowana obsługa iSCSI	Obsługa wielu jednostek LUN na Target Obsługa mapowania i maskowania LUN Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S Wykonywanie migawek oraz kopii zapasowej LUN
Obsługa Fiber Channel (FC SAN)	Wsparcie opcjonalnych kart FC Mapowanie LUN
Zarządzanie prawami dostępu	Przypisanie pojemności dla użytkowników Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie uprawnieniami dla użytkowników i grup Obsługa zaawansowanych uprawnień dla podfolderów
Obsługa Windows AD	Logowanie użytkowników domenowych poprzez protokoły CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera i klienta LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa plików, opracowane przez producenta urządzenia dla systemów Windows. Backup na zewnętrzne dyski twarde.
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Amazon S3, Amazon Glacier, Microsoft Azure, Google Cloud Storage, Dropbox, OneDrive for Business, Google Drive

Darmowe aplikacje na urządzenia mobilne	Monitoring i zarządzanie urządzeniem Współdzielenie plików Obsługa kamer Dostępne na systemy iOS oraz Android
Minimum obsługiwane aplikacje	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer pobierania (Bittorrent/HTTP/HTTPS/FTP)
VPN	VPN client / VPN server Minimum obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail Powiadamianie przez SMS (z wykorzystaniem zewnętrznych usług) DDNS oraz zdalny dostęp w chmurze producenta SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP oraz lokalnych przez USB Monitorowanie zasobów urządzenia Monitorowanie zasobów systemu w czasie rzeczywistym Rejestr zdarzeń Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Możliwość aktualizacji oprogramowania z powiadomieniem z serwerów producenta Ustawienia systemowe: kopia zapasowa, przywracanie, resetowanie systemu
Wirtualizacja	Możliwość uruchomienia maszyn wirtualnych z systemem Windows, Linux, Unix i Android Import maszyn wirtualnych Klonowanie maszyn wirtualnych Migawki maszyn wirtualnych
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem połączeń Obsługa HTTPS Obsługa SFTP Szyfrowanie AES 256-bit Import certyfikatu SSL

Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami producenta i aplikacjami firm zewnętrznych Możliwość instalacji z gotowych paczek oraz wbudowane narzędzia wirtualizacji umożliwiającee zarówno obsługę kontenerów Docker/LXC jak i pełnych maszyn wirtualnych
Gwarancja	3 lata

3.1.15.3. Parametry minimalne dla systemu bezpieczeństwa

Wymagania funkcjonalne dla Systemu.

1. System musi zawierać narzędzia do zautomatyzowanego tworzenia elektronicznej, interaktywnej dokumentacji infrastruktury teleinformatycznej uwzględniając schematy architektury zabezpieczeń sieci tzn. mapy pokazującej urządzenia zabezpieczeń, strefy bezpieczeństwa, zasoby teleinformatyczne, połączenia i topologię sieci LAN/WAN, prezentującej informacje nt. bezpieczeństwa w ujęciu technicznym oraz w odniesieniu do procesów działania organizacji.
2. System musi zawierać bazę wiedzy eksperckiej (tzw. Knowledge Base) uwzględniającej wiedzę, która pozwoli ocenić poprawność projektu zabezpieczeń, identyfikując efektywność zastosowanych mechanizmów sieciowych oraz lokalnych w stosunku do potencjalnych wektorów ataków oraz w przypadku ich niezastosowania zidentyfikować ryzyka, które się z tym wiążą.
3. Dostarczone rozwiązanie musi być systemem klasy SIEM (Security Information Event Management), do którego głównych funkcji należą gromadzenie i korelacja zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł, agregację i wzbogacanie danych. Korelacja odbywa się na podstawie zdefiniowanych reguł określających te zależności.
4. Interfejs systemu elektronicznej dokumentacji musi umożliwiać wizualizację informacji o infrastrukturze teleinformatycznej. Wizualizacja musi obejmować interaktywną mapę logiczną sieci z zaznaczonymi strefami sieci, strefami bezpieczeństwa, urządzeniami sieciowymi, połączeniami, systemami zabezpieczeń IT oraz procesami.
5. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji infrastruktury IT również w formie tabelarycznej.
6. System musi prezentować techniczne informacje nt. bezpieczeństwa IT z perspektywy działalności organizacji, w tym zapisywanie, wyszukiwanie i prezentowanie co najmniej następujących informacji: procesy biznesowe organizacji oraz wspierające je usługi i powiązane z nimi zasoby IT, klasyfikacja zbiorów informacji przetwarzanych w ramach wskazanych procesów oraz przez wskazane zasoby IT, ważność zasobów IT dla organizacji ze względu na typ przetwarzanych danych oraz wspierane procesy, właścicieli zasobów (Owners) oraz zespół IT odpowiedzialny za jego obsługę (Custodians).
7. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny (minimum: na podstawie danych pozyskanych z logów oraz poprzez API) lub za pomocą interfejsu graficznego i tabelarycznego.

8. Interfejs interaktywnej mapy sieci musi umożliwiać wyświetlanie i modyfikowanie szczegółowych informacji o każdym elemencie infrastruktury IT oraz posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT, który został zdefiniowany w elektronicznej dokumentacji.
9. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci.
10. System musi pozwalać na dodawanie i przechowywanie załączników powiązanych z obiektami zgromadzonymi w bazie elektronicznej dokumentacji sieci. System powinien akceptować załączniki między innymi w formatach: pdf, MS Word, MS Excel, jpg, png.
11. Dla zdarzeń zawierających adresy IP interfejs musi umożliwiać wyświetlenie dodatkowych informacji o zasobach powiązanych z tymi adresami m.in.: nazwa zasobu, rodzaj zasobu, powiązane usługi, właściciel zasobu, podatności zasobu, powiązane incydenty, lokalizacja.
12. System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego.
13. Dla zarejestrowanych zdarzeń/ incydentów system automatycznie wyznaczy ścieżkę ataku i zaprezentuje ją w formie graficznej na schemacie sieci organizacji. Ścieżka ataku pokazuje wszystkie urządzenia zabezpieczeń na drodze pomiędzy celem a źródłem zdarzenia lub incydentu.
14. Dla zdarzeń zawierających adresy IP interfejs musi umożliwiać wyświetlenie dodatkowych informacji o zasobach powiązanych z tymi adresami m.in.: nazwa zasobu, rodzaj zasobu, powiązane usługi, właściciel zasobu, powiązane incydenty, lokalizacja.
15. Informacje o procesach muszą uwzględniać ważność procesów dla organizacji, typy danych przetwarzanych w ramach procesów (np. dane osobowe, informacje poufne itp.), właścicieli procesów, relacje między procesami (np. proces A zależy od procesu B, przy czym zależności powinny być prezentowane w formie graficznej) oraz czas trwania procesów (np. proces praca biurowa w organizacji jest aktywny od poniedziałku do piątku od 8:00 do 16:00).
16. System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet).
17. W ramach obsługi zdarzeń/incydentów system powinien prezentować informacje o wynikach szacowania ryzyka dla zasobów związanych z incydentem oraz ocenę wpływu incydentu na organizację w przypadku materializacji zagrożenia.
18. System musi pozwalać na zautomatyzowane szacowanie ryzyka dla wszystkich systemów IT zdefiniowanych w elektronicznej dokumentacji. Szacowanie ryzyka powinno odbywać się względem zagrożeń natury informatycznej, np.: przełamanie zabezpieczeń, wyciek danych, infekcja złośliwym programem, podsłuch sieciowy.

19. System w razie wykrycia incydentów o wysokim ryzyku materializacji zagrożenia natury technicznej (m.in. przełamanie zabezpieczeń, infekcja złośliwym oprogramowaniem) umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email i SMS.
20. System w razie wykrycia incydentów o poważnych konsekwencjach dla organizacji umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email i SMS.
21. System powinien umożliwiać automatyczne wyszukiwanie pojedynczych, potencjalnych punktów awarii sieci i systemów IT, których uszkodzenie może spowodować zablokowanie krytycznych usług w organizacji.
22. System ma posiadać narzędzia do modelowania zagrożeń, umożliwiając symulowanie potencjalnych scenariuszy bezpieczeństwa. Interfejs mapy sieci musi pozwalać m.in. na:
    a. wyznaczenie źródła zagrożenia zasobu teleinformatycznego wraz z wynikiem analizy ryzyka dla tego zagrożenia wyliczanym w sposób automatyczny,
    b. wyświetlanie zabezpieczeń zasobu teleinformatycznego przed potencjalnymi źródłami zagrożenia,
    c. wyświetlanie zabezpieczeń chroniących zasoby teleinformatyczne przed określonym źródłem zagrożenia,
    d. wyświetlanie lokalizacji zasobów określonego rodzaju,
    e. wyświetlanie najbardziej narażonych zasobów teleinformatycznych,
    f. wyświetlanie ważnych zasobów teleinformatycznych narażonych na awarie.
23. System musi umożliwiać uwzględnianie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej w mechanizmach korelacji zdarzeń. Wykryte zdarzenia/ incydenty będą priorytetyzowane w odniesieniu do ważności dla organizacji zasobów, których dotyczą (np.: wspomaganych procesów, przetwarzanych informacji klasyfikowanych).
24. Rozwiązanie musi umożliwić korelację zdarzeń pochodzących z różnych urządzeń, punktów końcowych i aplikacji z anomaliami wykrywanymi w przepływach sieciowych oraz podatności pozyskanych bezpośrednio ze skanerów aplikacyjnych i bazy CVE.
25. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
26. System musi umożliwiać wykorzystanie baz reputacyjnych w regułach korelacyjnych.
27. System musi umożliwiać automatyczne dodawanie i usuwanie list referencyjnych na podstawie reguł korelacyjnych umożliwiających zdefiniowanie warunków na podstawie których listy te będą modyfikowane. System musi umożliwiać definiowanie list referencyjnych łączących unikalne wartości w pojedynczym wierszu np: login, adres IP, Aplikacja.
28. System musi być wyposażony w mechanizmy reguł opartych na mechanizmach behawioralnych z możliwością agregacji danych oraz punktowania poszczególnych zdarzeń w wyznaczonych oknach czasowych. W rezultacie działania reguł behawioralnych, system powinien tworzyć incydenty związane z przekroczeniem dozwolonych zakresów punktacji dla zdarzeń zaobserwowanych w oknie czasowym agregacji.
29. System musi zapewnić graficzny interfejs wspierający proces obsługi incydentów, którego zadaniem będzie wspieranie użytkownika w realizacji zadań związanych z selekcją zdarzeń, analizą incydentów, oceną wpływu i reakcją na incydenty. Do zadań tych należą między innymi:
    a. wzbogacanie danych kontekstowych,

b. gromadzenie artefaktów danych związanych z incydentem,
c. współpraca z innymi członkami zespołu,
d. komunikacja w ramach zespołu,
e. wykonywanie czynności związanych z reakcją na incydent,
f. raportowanie przebiegu incydentu.

30. 30. System musi być wyposażony w graficzny interfejs prezentujący w formie wykresów dane statystyczne związane z procesem obsługi incydentów. Wykresy muszą umożliwiać prezentację danych uwzględniających co najmniej: ilość incydentów w czasie w podziale na priorytety, czasy reakcji i obsługi oraz bieżące ilości incydentów obsługiwanych przez poszczególnych użytkowników.
31. System musi umożliwiać zbieranie, przechowywanie i przypisywanie wskaźników kompromitacji (IoC) do incydentów.
32. System powinien udostępniać automatyczny raport z wszystkich podjętych działań w ramach incydentu.
33. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych danych przez ich podział na pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie danych. Mechanizm musi umożliwiać m.in. parsowanie warunkowe, parsowanie hierarchiczne, wzbogacanie zdarzeń o dodatkowe pola, mapowanie wartości, czy wykorzystanie gotowych parserów przy tworzeniu nowych.
34. Parsowanie warunkowe i hierarchiczne musi być konfigurowalne i obsługiwać następujące metody normalizacji: REGEX, JSON, XML, CEF, LEEF, SYSLOG. Musi umożliwiać wykorzystanie gotowych parserów jako elementów podrzędnych hierarchii oraz wykorzystywanie ich w warunkach.
35. Proces normalizacji musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.
36. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.
37. System musi zapewnić normalizację (parsowanie) logów protokołami Syslog, TLS Syslog, Netflow, obsługiwać pliki płaskie (ang. flat file), zapytania do bazy danych poprzez sterownik ODBC oraz odbierać wiadomości email.
38. Oferowane rozwiązanie powinno zapewniać możliwość zbierania logów z systemów Microsoft Windows poprzez mechanizm Windows Event Forwarding (WEF) bez konieczności instalowania dedykowanego oprogramowania w tych systemach.
39. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.
40. Normalizacja musi uwzględniać możliwość nadawania kategorii zdarzeń na podstawie wartości parsowanych pól, np. logowanie, wylogowanie, zmiana uprawnień, malware, vulnerability.
41. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.
42. System musi posiadać predefiniowany zestaw parserów.
43. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) logów z niestandardowych źródeł danych, w oparciu o składnię wyrażeń regularnych oraz formaty JSON, XML, CIS, LEEF, Syslog. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia.

44. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.
45. System musi umożliwiać definiowanie zakresu i czasu uczenia, np.: analiza logowania użytkowników po godzinach pracy, analiza alarmów systemu SIEM. Po wdrożeniu nie będzie wymagane żadne dostrojenie systemu.
46. System musi mieć możliwość wzbogacania kontekstu odbiegającego od normalnego zachowania użytkownika korzystając z danych zewnętrznych, minimum: Threat Intelligence, Active Directory. Przykładowe zastosowanie integracji zakłada wykorzystanie zasobów zewnętrznych, z których dane mogą podnieść skumulowaną ocenę ryzyka dla sesji użytkownika.
47. System musi posiadać funkcję „automatycznej korelacji", tzn. posiadać zaszyte mechanizmy i reguły korelacji, które po wdrożeniu i „nauce środowiska zamawiającego", będą przedstawiać właściwe incydenty dla operatorów bez dodatkowej ingerencji w reguły.
48. System musi zapewniać możliwość budowania modeli zachowania użytkowników dla zebranych danych historycznych ze skonfigurowanego (wskazanego) okresu.
49. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych.
50. Dostarczone rozwiązanie musi być objęte 12 miesięcznym wsparciem producenta lub producentów. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania oraz reagowanie na zgłaszane błędy systemowe. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędu krytycznego lub poważnego).
51. Rozwiązania SIEM, narzędzia elektronicznej dokumentacji, oraz baza wiedzy mogą być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli.
52. Interfejs użytkownika Systemu musi być w języku polskim lub umożliwiać wgranie plików językowych tłumaczących interfejs na język polski. Musi być przejrzysty i konfigurowalny, poprzez pogrupowanie zawartości w bloki tematyczne, co ma umożliwić łatwe i szybkie wyszukiwanie odpowiednich danych.
53. Funkcjonowanie rozwiązania musi być oparta w całości o architekture „on-premise", w której przetwarzane dane nie są przesyłane poza infrastrukturę Zamawiającego.
54. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).
55. Dopuszczalne jest dostarczenie rozwiązania jako tzw. wirtualnego appliance pod warunkiem że obraz appliance jest udostępniany do pobrania przez producenta dostarczonego rozwiązania na jego oficjalnej stronie internetowej w postaci utwardzonego rozwiązania, łącznie z dedykowanym systemem operacyjnym, dla którego Producent regularnie dostarcza aktualizacje, w tym poprawki bezpieczeństwa.
56. System musi zapewniać możliwość współpracy z popularnymi bazami danych, a w tym co najmniej z: MS SQL lub Oracle.
57. System powinien umożliwiać nadawanie uprawnień do obiektów/modułów systemu dla poszczególnych operatorów lub grup operatorów.

58. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.
59. System musi dokonywać automatycznej integracji z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach i zasobach zarejestrowanych w domenie AD, minimum to: nazwa użytkownika, login, e-mail, nazwa komputera, przynależność do grup, przełożonego, jednostkę organizacyjną oraz konta uprzywilejowane.
60. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.
61. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień do definiowalnych grup odbiorców (co najmniej: powiadamianie email oraz SMS, opcjonalnie czat).
62. System musi być dostępny z poziomu dedykowanego klienta aplikacji lub obsługiwany za pomocą dowolnej przeglądarki internetowej (Chrome, Edge, Firefox), bez konieczności instalowania jakichkolwiek dodatków dla prawidłowego jego działania.
63. System musi umożliwiać przypisanie poziomów krytyczności do monitorowanych zasobów, które będą brane pod uwagę w ewaluacji zagrożeń.
64. System musi umożliwiać mapowanie zdarzeń korelacyjnych na framework Mitre ATT&CK.
65. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych danych w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne.
66. Tworzenie raportów PDF musi posiadać opcje automatycznego harmonogramu, który w zadanym wcześniej momencie pozwoli na wysyłkę utworzonego raportu do zdefiniowanych odbiorców poczty email. Konfiguracja harmonogramu tworzenia raportów PDF i ich wysyłki powinna być dostępna poprzez graficzny interfejs użytkownika.
67. System musi rejestrować i przechowywać pozyskane dane w wersji pierwotnej oraz w wersji znormalizowanej.
68. System musi zapewniać klasyfikację zdarzeń za pomocą notacji punktowej definiującej ich poziom zagrożenia (ryzyko).
69. Interfejs systemu powinien umożliwiać z poziomu jednego okna widoku weryfikację wszystkich działań użytkownika na osi czasu, które spowodowały wzrost ryzyka. Z poziomu tego widoku system umożliwi przejście do opisu konkretnego zdarzenia.
70. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa, m.in. usługi zagrożone przez incydenty, średni czas obsługi incydentu.
71. System pozwoli na prezentację danych w postaci tzw. „Dashboard”, tj. dostosuje zakres i prezentacje danych do potrzeb administratora czy też zalogowanego użytkownika.
72. System musi automatycznie wyodrębnić konta użytkowników oraz ich kontekst, minimum przynależność do odpowiednich grup domenowych, konta serwisowe, użytkowników

uprzywilejowanych, użytkowników w randze kierowniczej i zarejestrowane stacje robocze celem automatycznej dystrybucji tych danych do odpowiednich narzędzi systemu.

73. System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
74. System musi umożliwiać przechowywanie teczek incydentów zawierających dowody, próbki, logi oraz inne powiązane z danym incydentem informacje.
75. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody w teczkach Incydentów.
76. System musi umożliwiać powiązanie każdego zdarzenia/incydentu z odpowiednim priorytetem (definiowanym automatycznie z możliwością manualnej zmiany).
77. System powinien posiadać możliwość rejestracji zgłoszeń i przekształcenia ich w incydenty bezpieczeństwa z możliwością rozdzielenia uprawnień dla obu tych czynności.
78. System powinien mieć logikę automatycznego przypisywania zgłoszeń, minimum na podstawie dostępności operatora, jego obciążenia, oraz cech zasobu którego dotyczy incydent, minimum typ zasobu (np.: serwer lub stacja robocza), krytyczność oraz realizowane z jego udziałem usługi z katalogu usług.
79. System musi umożliwiać grupowanie manualne w jeden incydent bezpieczeństwa zdarzenia podobne/powiązane np. wielokrotnie raportowane, przez systemy źródłowe, wielokrotnie zgłoszone przez użytkowników.
80. System powinien grupować automatycznie w jeden incydent bezpieczeństwa zdarzenia podobne/powiązane np. wielokrotnie raportowane, przez systemy źródłowe, wielokrotnie zgłoszone przez użytkowników.
81. System powinien umożliwiać obsługę tzw. lawinowych incydentów (incydenty takie same, lecz pochodzące od różnych użytkowników lub systemów) poprzez podłączanie ich do jednego głównego incydentu oraz nadanie odpowiedniego priorytetu tego typu zdarzeniom. Zamknięcie głównego incydentu/zdarzenia powinno umożliwiać zamykanie powiązanych z nim incydentów/zdarzeń w trybie manualnym (operator) lub automatycznym (system). W podglądzie incydentu powinna się pojawić informacja o podpiętych incydentach.
82. System SIEM oraz wszystkie moduły towarzyszące muszą umożliwiać równoczesną pracę co najmniej 10 operatorów oraz objąć monitoringiem min. 500 zasobów IT. Przez zasób IT rozumie się serwery fizyczne lub serwery wirtualne oraz komputery użytkowników. Ilość danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz ilość kolektorów agregujących i parsujących nie może powodować zmian w zakresie licencjonowania. Wykonawca udzieli Zamawiającemu wieczystej, nieograniczonej czasowo licencji na zakupiony System.
83. System ma gwarantować możliwość elastycznej rozbudowy o dalsze zasoby IT, które w przyszłości zostaną objęte jego działaniem.
84. Zamówienie realizowane będzie w okresie 18 miesięcy od dnia zawarcia umowy, zgodnie ze wzorem umowy. Wykonanie zamówienia zostanie podzielone na etapy:
    a. Etap I – wdrożenie – w terminie do 6 miesięcy od dnia zawarcie umowy. Szczegółowy zakres i wytyczne Etapu I określa Załącznik nr 1;
    b. Etap II – utrzymanie i wsparcie systemu – w okresie 12 miesięcy, od dnia podpisania protokołu odbioru.

85. Po zakończonym wdrożeniu należy zapewnić bezpłatne certyfikowane szkolenia (5 x 8h) w zakresie użytkowania i administrowania wdrożonego systemu lub systemów dostarczonych w ramach zamówienia. Szkolenie ma zostać przeprowadzone dla maksymalnie 8 osób i uwzględniać informacje z zakresu wdrożonego systemu SIEM (m.in. zarządzanie incydentami bezpieczeństwa; kompletowanie informacji potrzebnych do opracowania raportu o incydencie; szacowanie ryzyka itp.). Szkolenia muszą być zakończone egzaminem i certyfikatem potwierdzającym wspomniane umiejętności wydanym przez producenta systemu. Szkolenia mogą odbyć się w formie zdalnej.
86. Wykonawca przekaże Zamawiającemu wszelkie, niezbędne do poprawnego korzystania z wdrożonego rozwiązania, informacje o specyfice systemu oraz informacje techniczne na temat jego prawidłowej eksploatacji (tj. szczegółową dokumentację powdrożeniową oraz instrukcję/instrukcje obsługi).

3.1.15.4. Szczegółowy zakres i wytyczne procesu wdrożenia systemu bezpieczeństwa

1. Proces wdrożenia systemu określony w Etapie I powinien zostać zrealizowany zgodnie z opisanymi niżej wytycznymi, umożliwiając efektywne wdrożenie rozwiązania w okresie 6 miesięcy.
2. Proces wdrożeniowy podzielony zostanie na 2 obszary:
   a. Obszar Analizy, zakładający stworzenie elektronicznej dokumentacji organizacji wraz z podłączeniem i skonfigurowaniem mechanizmów szacowania ryzyka pod kątem kluczowych zasobów IT i procesów organizacji (budowa kontekstu organizacji);
   b. Obszar Detekcji, zakładający podłączenie i konfigurację narzędzi odpowiedzialnych za wykrywanie zdarzeń i incydentów bezpieczeństwa w ramach zainstalowania modułu SIEM;
3. Obszar Analizy ma na celu identyfikację potencjalnych cyber zagrożeń oraz możliwych konsekwencji na jakie narażona jest organizacja. Zakres prac powinien uwzględniać kolejno:

a. Pracę z konsultantem (w zakresie m.in. wprowadzenia do metodyki oraz uzupełnienia ankiety przedwdrożeniowej);
b. Uruchomienie systemu w infrastrukturze zamawiającego, w tym:
- konsultacje w przygotowaniu infrastruktury zamawiającego do instalacji systemu,
- instalację lub import maszyny wirtualnej typu „software appliance”,
- zestawienie połączenia zdalnego,
- aktywację licencji,
- wstępną konfigurację,
- import/wprowadzenie tabeli adresacji znaczących stref bezpieczeństwa, wymaganych przez mechanizmy wykrywania (np.: sieci serwerów, sieci DMZ, sieci LAN);

c. Podłączenie głównego źródła zdarzeń opisującego komunikację sieciową, w tym:
- przekierowanie logów opisujących transmisje sieciową (traffic) z zapór sieciowych (Firewall) na kolektor systemu,
- uruchomienie reguł wykrywania;

d. Prace audytowe, w tym:
- pasywną analizę transmisji sieciowej:
  - ruch z/do serwerów webowych i aplikacyjnych,
  - ruch z/do serwerów baz danych,
  - ruch z/do serwerów pocztowych,
  - ruch z/do kontrolerów domenowych,

o ruch z/do serwerów usług podstawowych (m.in. DNS/NTP),

o ruch z/do zasobów zidentyfikowanych na bazie charakterystyki i wolumenu ruchu oraz możliwości identyfikacji aplikacji,

- konsultacje w ramach otrzymanych wyników;
- zebranie danych audytowych wymaganych do sporządzenia raportu;

e. Analizę podatności, w zakresie:

- integracji po API ze wskazanym przez zamawiającego komercyjnym skanerem/ skanerami podatności lub zainstalowanie skanera podatności typu open source;
- przygotowanie reguł priorytetów i importu krytycznych podatności;

f. Przygotowanie dynamicznego raportu audytowego w oparciu o dostępne w systemie narzędzia elektronicznej dokumentacji i szacowania ryzyka obejmującego analizę prawdopodobieństwa przełamania zabezpieczeń organizacji. Raport powinien zawierać:

- zidentyfikowane zagrożenia oraz prawdopodobieństwo ich wystąpienia;
- potencjalne wektory ataków dla wykrytych zagrożeń;
- wizualizacja graficzna wykrytych źródeł zagrożeń oraz wektorów ataków;
- rekomendacja zabezpieczeń;
- zidentyfikowane zagrożenia związane z podatnościami oraz prawdopodobieństwo wykorzystania ich do przełamania zabezpieczeń;

g. Transfer wiedzy w formie spotkania podsumowującego, obejmujący interpretację przez analityka wyników analizy ujętej w raporcie z systemu;

4. Obszar Detekcji ma na celu uruchomienie i dostrojenie mechanizmów wykrywania zagrożeń. Zakres prac powinien uwzględniać kolejno:

a. Podłączenie (przekierowanie do systemu) źródeł zdarzeń i ich dalszą konfigurację. Kluczowe źródła zdarzeń obejmują:

- zapory sieciowe w punkach styku z siecią Internet (Firewall brzegowy);
- sieciowe systemy bezpieczeństwa dedykowane do wykrywania incydentów bezpieczeństwa (np.: Sandbox, IDP/IPS, AntySpam)
- centralne systemy, dedykowane do kontroli złośliwego oprogramowania na stacjach końcowych/Serwerach, umożliwiające wykrywanie aktywności złośliwego oprogramowania (np.: AntyWirus, EDR);
- kontroler domenowy oraz system zarządzania dostępem uprzywilejowanym;
- systemy detekcji anomalii w przepływach lub zdarzeniach (np.: NBA);
- system SIEM
- w przypadku niestandardowych źródeł, muszą zostać przygotowane odpowiednie parsery, pozwalające na detekcję zgodną z wbudowanymi w system regułami korelacji;

b. Adaptację reguł profilowych, pozwalających na dostosowanie zdarzeń do zasobów, których dotyczą;

c. Podłączenie reguł detekcji;

d. Podłączenie i konfiguracja mechanizmów UEBA:

- integracja z Active Directory
- utworzenie profili użytkowników UBA
- utworzenie profili hostów EBA
- import reguł bezpieczeństwa UEBA, utworzenie customowych reguł bezpieczeństwa UEBA, uruchomienie procesu uczenia
- obserwacja i doprecyzowanie postępu uczenia maszynowego, wykluczenie/ dodanie nowych reguł zdarzeń użytkowników/ hostów.

c. Dostrojenie systemu, w tym reguł priorytetyzacji zdarzeń i incydentów, mające na celu dopasowanie czułości systemu do możliwości operacyjnych organizacji;

3. 1.16 Wykonanie połączeń światłowodowych z urządzeniami WiFi

Należy wykonać planowanie radiowe oraz w zgodzie z tym planowaniem umieścić połączenia do urządzeń WiFi do najbliższego węzła PD.

4. Warunki realizacji projektu

4.1. Etapy realizacji

Tabela 2 Tabela etapów realizacji projektu

Etap	Zakres prac zgodnych z tabelą OPZ	Termin zakończenia etapu
I	Wykonanie i dostarczenie dokumentacji projektowej	Nie dłużej niż 40 dni od daty podpisania umowy
II	Budowa serwerowni oraz okablowania strukturalnego	Wg zapisów z dokumentacji projektowej
III	Dostawa i instalacja sprzętu serwerowni	Wg zapisów z dokumentacji projektowej
IV	Testy i uruchomienie	Wg zapisów z dokumentacji projektowej
V	Szkolenia	Nie dłużej niż 20 dni od daty odbiory etapu II
VI	Odbiór końcowy oraz rozpoczęcie świadczenia usług serwisowych	Do 10 dni od daty zakończenia etapu IV lecz nie dłużej niż do 10.12.2022 roku.

Dopuszcza się realizację odbioru poszczególnego etapu warunkowo, jeżeli wstrzymywały by to pracę następnego etapu, pod następującymi warunkami łącznie:

1. Jeżeli odbiór znacząco opóźnił by cały projekt a bez oddania etapu w całości można rozpocząć pracę nad następnym etapem,
2. Do ukończenia etapu zostało nie więcej jak 10% prac,
3. Odbiór etapu nastąpi nie później niż odbiór etapu kolejnego.
4. Szkolenia nie wstrzymują daty odbioru i mogą się odbyć w formie vouchera terminowego gdzie termin może wybiec poza datę odbioru projektu.

Dni harmonogramu liczy się jako dni kalendarzowe.

4.2. Przygotowanie dokumentacji

1. W początkowym stadium realizacji projektu, w terminie określonym harmonogramem, Wykonawca opracuje w uzgodnieniu z Zamawiającymi dokumentację projektową.

2. Dokumentacja wraz z SIWZ będą stanowiły podstawę do weryfikacji funkcjonalnej i jakościowej w trakcie odbiorów końcowych.
3. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiających. Akceptacja Dokumentacji warunkuje rozpoczęcie prac Wykonawcy.
4. Podczas opracowania DPR Wykonawca może zmienić karty katalogowe będące częścią DAP (jeżeli dotyczy). Zmiana ta wymaga każdorazowej akceptacji Zamawiającego.

4.3. Warunki realizacji części sprzętowej i instalacyjnej

1. Zamawiający na wniosek Wykonawcy dopuszcza przed przystąpieniem do sporządzania oferty wizję lokalną celem weryfikacji założeń do kosztorysu (samodzielnej weryfikacji prac koniecznych do wykonania, tj. przeloty, odwierty w ścianach działowych, stanu serwerowni i punktów dystrybucyjnych itp. - dla prawidłowego oszacowania czasu realizacji, oszacowania poziomu trudności prac i ilości koniecznych do zastosowania materiałów). W tym celu należy kontaktować się z Zamawiającym.
2. Zamawiający określił niezbędną ilość poszczególnych elementów rozbudowywanej sieci strukturalnej w poszczególnych lokalizacjach, do zweryfikowania na etapie projektowania po dokonaniu stosownych ustaleń z Zamawiającym i administratorem. Zestawienie wymagań dla materiałów dla sieci strukturalnej opisane jest rozdziale poniżej niniejszego opracowania. Wykonawca powinien stosować się do ww. wymagań podczas wykonywania prac, uwzględniając wytyczne Zamawiającego co do rozmieszczenia poszczególnych elementów sieci, a także zweryfikować je pod kątem stworzonej Dokumentacji Projektowej. W tym zakresie do współpracy z Wykonawcą oddelegowany zostanie pracownik Zamawiającego.
3. Wykonawca dostarczy Zamawiającemu komplet Dokumentacji Projektowej i Powykonawczej.
   a. Dokumentacja Projektowa musi zawierać informacje ogólne (temat projektu, jego zakres, uwagi), ogólną koncepcję rozwiązań technicznych i funkcjonalnych, opis parametrów technicznych urządzeń, materiałów i oprogramowania, szczegóły rozwiązań technicznych, wykaz testów adaptacyjnych, wykaz urządzeń, materiałów, schematy instalacyjne, elektryczne i logiczne.
   b. Dokumentacja Powykonawcza musi zawierać opis faktycznego stanu rzeczy wraz z protokołami pomiarów wszystkich torów łączności oraz testami zabezpieczenia nadmiarowo-prądowego, przepięciowego, różnicowo-prądowego, oporności uziomu ochronnego itp. W części Dokumentacji Powykonawczej, dotyczącej sieci bezprzewodowej Wykonawca umieści wyniki z przeprowadzonych pomiarów propagacji sygnału sieci bezprzewodowej 802.11 w zakresie częstotliwości 2.4 i 5GHz wraz z naniesionymi punktami na planach gdzie zamontowana zostaną urządzenia Access Point oraz schematami połączeń (okablowanie) prowadzących do najbliższych punktów PD.
   c. Zamawiający wymaga dostarczenia Dokumentacji Projektowej i Powykonawczej w formie wydruku i wersji na nośniku elektronicznym. Część opisowa: edytor tekstu, część rysunkowa: na podkładach budowlanych w formacie dwg lub zgodnym oraz w formacie pdf.
4. Wykonawca wykona wszelkie prace adaptacyjne i przystosowawcze w pomieszczeniach i miejscach, w tym demontaż istniejącej sieci (w miejscu instalacji nowej sieci), w których będzie budowane/rozbudowywane okablowanie strukturalne na podstawie uzgodnień i uwag z

ewentualnej wizji lokalnej, oraz zgodnie z Dokumentacją zatwierdzoną przez Zamawiającego przed podjęciem prac. Prace instalacyjne muszą być wykonywane etapami tak, aby zapewnić pełną funkcjonalność istniejącej infrastruktury teleinformatycznej, oraz żeby nie kolidowały z normalnym funkcjonowaniem obiektów. Godziny prac instalatorów sieci stanowią przedmiot odrębnych ustaleń z Zamawiającym.

5. Przed przystąpieniem do instalacji okablowania strukturalnego, (jeśli będzie to konieczne) należy wykonać lub poszerzyć przepusty pomiędzy kondygnacjami budynków i w ścianach pomiędzy pomieszczeniami.
6. Wszelkie uzasadnione zmiany, które Wykonawca chciałby wprowadzić do Dokumentacji (na etapie wykonawstwa) muszą być uzgodnione z Zamawiającym. Wszelkie prace budowlano-montażowe związane z realizacją niniejszego zadania należy wykonać zgodnie z obowiązującymi normami oraz wytycznymi technicznymi, a w szczególności przestrzegać przepisów BHP. Wszystkie wykonywane prace oraz proponowane materiały winny odpowiadać Polskim Normom i posiadać stosowną deklarację zgodności lub posiadać znak CE (Europa) i deklarację zgodności z normami zharmonizowanymi oraz posiadać niezbędne atesty tak aby spełniać obowiązujące przepisy, Wykonawca jest obowiązany do uzyskania odpowiedniego rezultatu końcowego. Wszelkie niezgodności, ewentualne braki lub niezgodności interpretacyjne dokumentacji w zakresie instalacji słaboprądowych należy uzgadniać z Zamawiającym.
7. Wyroby instalacyjne użyte do wykonania prac, mają spełniać wymagania polskich przepisów, a Wykonawca będzie posiadał dokumenty potwierdzające, że zostały one wprowadzone do obrotu zgodnie z regulacjami Ustawy o wyrobach budowlanych i posiadają wymagane parametry. Dokumenty te Wykonawca dołączy do Dokumentacji Powykonawczej. Zamawiający przewiduje bieżącą kontrolę wykonywanych robót budowlanych. Wykonawca jest odpowiedzialny za pełną kontrolę robót, jakość materiałów i elementów oraz zapewni odpowiedni system kontroli jakości.
8. Do Dokumentacji Powykonawczej należy dołączyć niezbędne pomiary.
9. Wykonawca dostarczy przed rozpoczęciem prac imienną listę osób wyznaczonych do prac na terenie obiektów objętych projektem wraz z niezbędnymi danymi identyfikacyjnymi (nr i seria dowodu osobistego). Dane te będą stanowiły podstawę do identyfikacji osób przebywających na terenie obiektu w trakcie trwania prac. Wszelkie zmiany w danych identyfikacyjnych osób upoważnionych ze strony Wykonawcy, jak i modyfikacje odnośnie samych osób należy niezwłocznie zgłosić Zamawiającemu. W przeciwnym wypadku osobom wyznaczonym do realizacji prac zostanie wstrzymany dostęp do pomieszczeń.
10. Wszystkie miejsca, w których będą prowadzone prace budowlane (rozkucia, przekucia, przewierty itp.) muszą zostać doprowadzone do stanu wizualnie zbieżnego z wyglądem miejsca otaczającego i nie mogą być w stanie pogorszonym (należy dokonać uzupełnień brakującego tynku i pomalować te miejsca w kolorze maksymalnie zbliżonym do otaczającego go miejsca). Po wykonaniu prac budowlano-instalatorskich pomieszczenia zostaną doprowadzone do stanu nie gorszego niż przed rozpoczęciem robot, co zostanie potwierdzone przez przedstawiciela Zamawiającego i jest warunkiem koniecznym do podpisania Protokołu odbioru końcowego. Listwy kablowe muszą być położone estetycznie, równo, muszą być zakryte na całej długości.
11. Elementy okablowania strukturalnego oraz sieci elektrycznej (o ile zaistnieje) mają zostać oznaczone zgodnie z wytycznymi Zamawiającego. Producent instalowanego systemu okablowania

strukturalnego musi spełniać wymagania jakościowe zarówno w zakresie działalności handlowej jak i zakresie działalności produkcyjnej. Należy zapewnić objęcie wykonanej instalacji gwarancją systemową producenta zgodnie z zapisami Umowy, gdzie okres gwarancji udzielony przez producenta nie może być krótszy niż 3 lata zgodnie z ofertą.

12. Okres gwarancji ma być standardowo udzielany przez producenta okablowania, tzn. na warunkach oficjalnych, ogólnie znanych, dostępnych i opublikowanych.
13. Wszelkie uszkodzenia infrastruktury ogólnej na obiekcie spowodowane przez Wykonawcę podczas prowadzenia robót obciążają jego samego i muszą być usunięte w ramach nieodpłatnego usunięcia szkód w terminie natychmiastowym po ich stwierdzeniu.
14. W okresie prowadzenia budowy i jej wykończenia Wykonawca zobligowany jest stosować się do przepisów i zasad zapewniających odpowiednie warunki wykonywania pracy i pobytu osób na terenie budowy, w tym także zapewniać poprawne oddziaływanie prowadzonych prac na środowisko, ze szczególnym uwzględnieniem przepisów BHP, ustawy o ochronie środowiska i ustawy o odpadach i stosownych przepisów wykonawczych. Zamawiający wymaga, aby Wykonawca we własnym zakresie zapewnił składowanie i sprzątanie odpadów.
15. Prace instalacyjne będą mogły być prowadzone w trakcie pracy szpitala, ale należy uwzględnić specyfikę pracy Zamawiającego.
16. Prace należy wykonywać w sposób taki aby infrastruktura obecnie pracująca mogła działać bez przerw.
17. Po przepięciu infrastruktury aktywnej starej na nową, stary sprzęt należy zdemontować.
18. Należy przenieść konfigurację istniejącej sieci na nową, (ponad 100VLAN z Traffic Shaping).
19. Istnieje możliwość magazynowania sprzętu po jego dostawie w pomieszczeniach szpitala.
20. Okablowanie PD krosujące należy wymienić, chyba, że istniejące okablowanie spełni parametry transmisyjne sieci.
21. Należy dostarczyć komplet patchcordów.
22. Liczba VLANów i SSID należy ustalić na etapie montażu z Zamawiającym.

4.4. Gwarancja i dostępność serwisu

Gwarancję po wdrożeniu projektu w Szpitalu, należy podzielić na gwarancję dla systemów informatycznych i na gwarancję dla sprzętu teletechnicznego. Wszelkie urządzenia bezpieczeństwa powinny posiadać okres działania z aktualnymi szczepionkami minimum 3 lat. Pozostały okres gwarancji to minimum 3 lata z tym, że dostępność serwisu powinna być nie mniej niż 5x8xNBD czyli 5 dni w tygodniu przez 8 godzin z czasem serwisu dla następnego dnia roboczego. Wykonawcą gwarancji powinien być producent, lub firma do tego upoważniona. zadaniem takiej firmy jest sprawowanie obsługi serwisowej oraz bieżącego nadzoru nad Sprzętem i Systemami, przez okres minimum 3 lata, co w szczególności oznacza:

1. stały nadzór nad wdrożoną infrastrukturą i systemem w zakresie zgodności funkcji istniejących na dzień zawarcia Umowy z obowiązującymi przepisami prawa dotyczącymi tych funkcji. Nadzór obejmuje zgodność z przepisami o randze co najmniej rozporządzenia, w rozumieniu art. 87 ust. 1 Konstytucji RP z dnia 2 kwietnia 1997 roku oraz obowiązującymi wykładniami prawnymi lub wskazówkami jednostek nadrzędnych (Urząd Komunikacji Elektronicznej i inne organy władzy i administracji rządowej i samorządowej);

2. przygotowywanie Aktualizacji (Upgrade'ów) w zakresie objętym nadzorem nad infrastrukturą i urządzeniami. Wykonawca rozpocznie prace mające na celu przygotowanie Aktualizacji (Upgrade'u) nie później niż w dniu opublikowania odpowiednich przepisów prawnych lub oprawek np. przy pamięci masowej i wykona je tak aby termin instalacji Aktualizacji (Upgrade'u) Systemu pozwalał na jej zastosowanie zgodnie z terminem wejścia w życie zmienionych lub nowych przepisów (w przypadku, gdyby termin opublikowania przepisów prawnych nie pozwalał na przygotowanie Aktualizacji (Upgrade'u) w tym terminie, Strony uzgodnią inny termin wprowadzenia zmian z uwzględnieniem możliwości realizacji w jak najkrótszym czasie);
3. proponowanie prac rozwojowych;
4. udostępnienie i zainstalowanie przez Wykonawcę Aktualizacji (Upgrade'ów) i Poprawek (Update'ów) bez obowiązku ponoszenia dodatkowych opłat z tego tytułu przez Zamawiającego;
5. przyjmowanie zgłoszeń Błędów blokujących, Błędów krytycznych oraz Usterek za pośrednictwem Systemu Obsługi Zgłoszeń w trybie 24 godziny przez 7 dni w tygodniu. Błędy blokujące prace będą dodatkowo (łącznie ze zgłoszeniem w elektronicznym systemie) zgłaszane w godzinach 16: 00 – 08: 00 na dyżurny numer „helpdesk";
6. usuwanie zgłoszonych przez Zamawiającego Błędów blokujących, Błędów krytycznych oraz Usterek, ujawnionych w trakcie eksploatacji Systemu;
7. diagnostyka, optymalizacja i serwis działania infrastruktury;
8. podejmowanie działań wyprzedzających w odpowiedzi na zgłoszenia z automatów monitorujących parametry krytyczne Systemu (monit) w zakresie nieprawidłowego działania infrastruktury;
9. informowanie Zamawiającego o nowych aktualizacjach Systemu;
10. udostępnianie Zamawiającemu wraz z nowymi wersjami Systemu (Aktualizacjami) dokumentacji technicznej

4.5. Wymagania dotyczące kompletności wykonania

1. Projekt składa się na budowę sieci, infrastruktury IT i wdrożenie oprogramowania.
2. Infrastruktura sieci i infrastruktura IT jest planowana na minimum 1.000 użytkowników i musi zostać tak zaplanowana aby tyle użytkowników obsłużyć.
3. Wykonawca musi posiadać odpowiedni status np. Licencjonowanego Przedsiębiorstwa do Projektowania i Instalacji, nadany bezpośrednio przez Producenta okablowania, potwierdzony umową, regulującą warunki udzielania gwarancji systemowej przez producenta.
4. Ponadto wykonawca ma dysponować osobami posiadającymi imienne dyplomy potwierdzające ukończenie kursów kwalifikacyjnych w zakresie: instalacji, pomiarów, nadzoru, wykrywania oraz eliminacji uszkodzeń, projektowania okablowania strukturalnego, zgodnie z normami międzynarodowymi oraz procedurami instalacyjnymi producenta okablowania.
5. Wszystkie elementy systemu okablowania miedzianego i światłowodowego powinny być opracowane (tj. zaprojektowane, wykonane i wdrożone do oferty rynkowej), jako kompletne rozwiązania, celem uzyskania maksymalnych zapasów transmisyjnych oraz zapewnić uzyskanie certyfikatu producenta okablowania.

6. Wszystkie urządzenia sieciowe muszą zostać dostarczone z pełną funkcjonalnością o nieograniczonym czasie działania, a jeżeli urządzenia te wymagają w tym zakresie licencji, Wykonawca musi dostarczyć licencję działania dla nich na minimum 10 lat.
7. Wymaga się, aby wszystkie elementy okablowania (w szczególności: panele krosowe, gniazda, kabel, kable krosowe, płyty czołowe gniazd, prowadnice kablowe) spełniały warunek zapewnienia uzyskania certyfikatu producenta okablowania.
8. System okablowania strukturalnego musi obejmować kompletne rozwiązanie dla techniki miedzianej i światłowodowej, telekomunikacyjnej oraz szaf teleinformatycznych wraz z osprzętem. Elementy systemu okablowania powinny szczególnie być nastawione na uniwersalność, skalowalność, łatwość w montażu oraz prostotę i przejrzystość całości rozwiązań.
9. Wszystkie komponenty systemu okablowania muszą być zgodne z wymaganiami obowiązujących norm: ISO/IEC 11801 2 Ed. oraz EN 50173 2.Ed co musi być potwierdzone odpowiednimi certyfikatami. Należy zapewnić również certyfikat z niezależnego laboratorium posiadającego odpowiednią akredytacje potwierdzający zgodność łącza klasy EA z normą ANSI/TIA-568-C.2 (2009-08) w zakresie testu łącza 2 konektorowego Permanent Link.
10. Wykonawca jest zobowiązany dostarczyć system zarządzania infrastrukturą sieci aktywnej przewodowej tak aby z jednego miejsca (pulpitu) dało się zarządzać tą infrastrukturą.
11. System zarzadzania może być systemem do zarzadzania urządzeniami sieci przewodowej i bezprzewodowej, ale też może być systemem oddzielnym realizującym zarządzanie siecią bezprzewodową z kontrolera, a urządzeniami sieci przewodowej z odpowiedniego serwera.

4.6. Warunki wykonania i odbioru instalacji sprzętowych

4.6.1. Wizja lokalna

Zamawiający dopuszcza wizję lokalną obiektu celem samodzielnej weryfikacji prac koniecznych do wykonania, tj. przeloty, modernizacji pomieszczenia Serwerowni.

4.6.2. Ogólne warunki wykonania i odbioru instalacji sprzętowych

1. Wymaga się od Wykonawcy konsultacji roboczych z Zamawiającym oraz zorganizowania spotkań w celu uściślenia przyjętych rozwiązań projektowych, standardu wykończenia i wyposażenia.
2. Udzielania wyjaśnień , uzupełnień do Dokumentacji Projektowej w terminie max do 3 dni od zgłoszenia przez Zamawiającego.
3. Stawiania się na obiekt na wezwanie Zamawiającego, przy czym wezwanie lub zawiadomienie powinno być przesłane (fax./e-mail) min. na 2 dni robocze przed terminem spotkania. W przypadku nie wywiązywania się z powyższego obowiązku Zamawiający, wynikłe z tego tytułu straty pokryje z zatrzymanego zabezpieczenia należytego wykonania umowy. Zamawiający nie będzie ponosił kosztów pobytu na budowie bez wezwania bądź na wezwanie Wykonawcy robót.
4. Opracowania i pobyty na miejscu realizacji zadania wynikające z poprawienia błędów i uzupełnienia dokumentacji stanowiącej podstawę do realizacji robót Wykonawca wykonuje nieodpłatnie.

4.6.3. Możliwe do wystąpienia utrudnienia w wykonywaniu prac instalacyjnych

1. Obiekt jest czynny.
2. W obiekcie całą dobę wykonuje swoje prace personel obsługi.
3. W obiekcie stale przebywają zaproszeni i pracownicy.
4. Czasowe ograniczenia w dostępie do pomieszczeń.
5. Ograniczenia i obostrzenia dotyczące zgody na prace hałaśliwe, uciążliwe i brudne.
6. Prace na wysokości.

4.7. Równoważność w zakresie sprzętowym

1. Gdziekolwiek w dokumentach kontraktowych przywołane zostaną konkretne normy i przepisy, które spełniać mają materiały, sprzęt i inne towary oraz wykonane i zbadane roboty, będą obowiązywać postanowienia najnowszego wydania lub poprawionego wydania przywołanych norm i przepisów o ile w warunkach kontraktu (umowy) nie postanowi się inaczej. W przypadku, gdy przywołane normy i przepisy odnoszą się do konkretnego kraju lub regionu, mogą być również stosowane inne odpowiednie normy zapewniające równy lub wyższy poziom wykonania niż przywołane normy lub przepisy, pod warunkiem ich sprawdzenia i pisemnego zatwierdzenia przez Zamawiającego. Różnice pomiędzy przywołanymi normami a ich proponowanymi zamiennikami muszą być dokładnie opisane przez Wykonawcę i przedłożone Zamawiającemu do zatwierdzenia.
2. Wyroby budowlane, stosowane w trakcie wykonywania robót budowlanych, lub instalacyjnych mają spełniać wymagania polskich przepisów, a Wykonawca będzie posiadał dokumenty potwierdzające, że zostały one wprowadzone do obrotu, zgodnie z regulacjami ustawy o wyrobach budowlanych i posiadają wymagane parametry.
3. Specyficzne wyroby budowlane wytwarzane według zasad określonych w Dokumentacji Projektowej lub w specyfikacjach technicznych będą wymagały przeprowadzenia badań potwierdzających, że spełniają one oczekiwane parametry. Koszty przeprowadzenia tych badań obciążają Wykonawcę, a potrzeba tych badań i ich częstotliwość określą specyfikacje techniczne.
4. Jeżeli dokumentacja projektowa, przedmiar lub specyfikacja techniczna wykonania i odbioru robót wskazywałaby w odniesieniu do niektórych materiałów i urządzeń znaki towarowe lub pochodzenie, Zamawiający, zgodnie z ustawą Pzp, dopuszcza składanie produktów równoważnych. Wszelkie produkty pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, jakim muszą odpowiadać towary, aby spełnić wymagania stawiane przez Zamawiającego i stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia. Poprzez zapis dot. minimalnych wymagań parametrów jakościowych Zamawiający rozumie wymagania towarów zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma na celu jedynie doprecyzowanie oczekiwanego przez Zamawiającego produktu i 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 parametrach wskazanych lub

lepszych. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, uwiarygodniających te materiały lub urządzenia.

5. Zamawiający dopuszcza składanie ofert zawierających rozwiązania równoważne. Wskazanie równoważności zaoferowanego rozwiązania spoczywa na Wykonawcy.
6. Wykonawca, który powołuje się na rozwiązania równoważne, jest zobowiązany wykazać, że oferowane przez niego materiały, urządzenia oraz ich elementy spełniają wymagania określone przez Zamawiającego, poprzez dołączenie kart charakterystyki technicznej, certyfikatów, katalogów, folderów, opisów technicznych oferowanego ww. elementu oraz uzyskać wszelkie ewentualne uzgodnienia.
7. Dopuszcza się stosowanie infrastruktury okablowania kategorii 6 w przypadku zapewnienia na odcinku pomiędzy urządzeniami bezprzerwowej i zmierzonej transmisji na poziomie minimum 1GE. Dopuszcza się możliwość wykorzystania okablowania istniejącego po inwentaryzacji i pomiarach okablowania.
8. Urządzenia WiFi muszą zostać dostarczone z nieograniczoną możliwością konfiguracji ponad 16 SSID w okresie dożywotnim, a jeżeli wymagana jest licencja w tym zakresie na minimum 5 lat.
9. Wszystkie urządzenia sieciowe muszą zostać dostarczone z pełną funkcjonalnością o nieograniczonym czasie działania, a jeżeli urządzenia te wymagają w tym zakresie licencji, Wykonawca musi dostarczyć licencję działania dla nich na minimum 10 lat.
10. W związku z powyższym, w przypadku zaproponowania rozwiązań równoważnych, Wykonawca powinien złożyć Zamawiającemu następujące dokumenty:
    a. Karta katalogowa urządzenia wraz z informacjami potwierdzającymi spełnienie oczekiwanych parametrów
    b. Opis techniczny zaoferowanego rozwiązania równoważnego.
11. Zachodzenia kanałów na siebie w ilości 3 dla pasma 2,4GHz. W skrajnym przypadku dopuszcza się zachodzenie na siebie kanałów przy prawidłowej współpracy z kontrolerem tj. nie zakłócaniu się.

4.8. Testy infrastruktury – metodyki i procedury

4.8.1. Procedura testowania

1. Procedura dotyczy testów funkcjonalnych Komponentów poprzedzających Odbiór komponentu, zgodnie z Harmonogramem wdrożenia.
2. Termin i czas przeprowadzenia poszczególnych testów funkcjonalnych zostanie określony w Harmonogramie wdrożenia.
3. Przygotowanie testów funkcjonalnych:

    a) Wykonawca w terminie uzgodnionym z Zamawiającym dla poszczególnych testów funkcjonalnych przekaże do akceptacji Zamawiającemu plan i zakres testów.

        i) Plan testów musi zawierać co najmniej:
            (1) proponowany czas trwania testu wraz z iteracjami,
            (2) podstawowe informacje na temat przedmiotu testów,
            (3) nazwę Komponentu, nazwę modułu, nazwę funkcjonalności,

(4) scenariusz testów danej funkcjonalności, wraz z informacją o konfiguracji (jeżeli jest wymagana dodatkowa), kryteria akceptacyjne.

b) Zamawiający wniesie ewentualne uwagi do przedstawionego planu testu w ciągu 7 dni roboczych.

c) Wykonawca uwzględni uwagi Zamawiającego oraz przekaże poprawiony plan testów w ciągu 3 dni roboczych.

d) Brak akceptacji planu testu uniemożliwia rozpoczęcie testów funkcjonalnych danego Komponentu.

4. Zakres testów funkcjonalnych, będzie odpowiadał zakresowi realizacji danego Komponentu w ramach danego etapu i będzie obejmować kompletność, poprawność instalacji i działania Przedmiotu Zamówienia w zakresie określonym w OPZ.
5. Przed przystąpieniem do testów funkcjonalnych Wykonawca jest zobowiązany przedstawić Dokumentację użytkową zgodną z wersją testowanego Komponentu.
6. Iteracje testów i reakcja na Wady w trakcie wykonywania testów funkcjonalnych:

e) Pierwsza iteracja testów:

i) w trakcie testów Zamawiający na bieżąco zgłasza Wady.

ii) po zakończeniu realizacji testów, Wykonawca przekaże Zamawiającemu protokół rozbieżności, zawierający Wady.

iii) czas usunięcia wszystkich Wad po pierwszej iteracji: do 5 dni roboczych od przekazania protokołu rozbieżności.

f) Druga iteracja testów - weryfikacja usuniętych Wad zgłoszonych w pierwszej iteracji testów:

i) w trakcie testów Zamawiający na bieżąco zgłasza Wady.

ii) po zakończeniu realizacji testów, Wykonawca przekaże Zamawiającemu protokół rozbieżności, zawierający Wady.

iii) czas usunięcia wszystkich Wad po drugiej iteracji: do 3 dni roboczych od przekazania protokołu rozbieżności.

g) Trzecia iteracja testów - weryfikacja usuniętych Wad zgłoszonych w poprzednich iteracjach testów:

i) w trakcie testów Zamawiający na bieżąco zgłasza Wady.

ii) po zakończeniu realizacji całego scenariusza testowego, Wykonawca przekaże Zamawiającemu protokół rozbieżności, zawierający Wady.

iii) czas usunięcia wszystkich Wad po trzeciej iteracji: do 2 dni roboczych od przekazania protokołu rozbieżności.

h) Czwarta iteracja testów - weryfikacja usuniętych Wad zgłoszonych w poprzednich iteracjach testów.

7. W sytuacji, gdy pomimo dokonania iteracji testów wskazanych w OPZ, testy nie zakończą się pomyślnie, a Wady są istotne – uniemożliwiające prawidłowe korzystanie z Przedmiotu Zamówienia Zamawiający może odstąpić od realizacji Umowy z przyczyn leżących po stronie Wykonawcy.
8. Zakończenie testów funkcjonalnych z wynikiem pozytywnym umożliwia Odbiór Komponentu, etapu, końcowy zgodnie z „Procedurą odbiorową” stanowiącą załącznik nr 2.02 do Umowy.

9. Wszelkie powiadomienia przez Strony, w trakcie testów funkcjonalnych, odbywać się będą w formie pisemnej z wykorzystaniem poczty elektronicznej w ramach ustalonego w Dokumentacji Analizy przedwdrożeniowej kanału komunikacyjnego.
10. Testy funkcjonalne Komponentu zakończą się Raportem z testów funkcjonalnych, który musi być przyjęty przez Zamawiającego bez zastrzeżeń.

4.8.2. Minimalny zakres Testów funkcjonalnych

1. Okablowanie Strukturalne
   a) Sprawdzenie zgodności z dokumentacją projektową
   b) Sprawdzenie wyników pomiarów na zgodność z dokumentacją producenta
   c) Sprawdzenie poziomu sygnału sieci wifi w wymaganych strefach na zgodność z dokumentacją

4.8.3. Testy infrastruktury

Po ukończeniu prac instalacyjnych Wykonawca zobowiązany jest do uruchomienia i przetestowania poprawności, oraz bezpieczeństwa działania całej infrastruktury sieci WLAN i przedstawienia wyników Zamawiającemu.

W razie wykrycia problemów, uszkodzeń niewynikających z wadliwego działania urządzeń dostarczonych przez Zamawiającego, wykonawca jest zobowiązany do usunięcia wszystkich usterek i ponownego przeprowadzenia testów.

Wynikiem wszystkich przeprowadzonych prac powinna być w pełni funkcjonująca infrastruktura sieci WLAN wykonana na podstawie wcześniej wykonanego projektu i ustaleń z Zamawiającym.

4.8.4. Procedura wymagana dla testu sieci WLAN:

1. Testy dostępu bezprzewodowego wykonane dla pasma 2.4 oraz 5GHz,
2. Potwierdzenie możliwości dostępu do sieci WLAN poprzez poszczególne SSID we wszystkich wymaganych obszarach obiektu,
3. Weryfikacja działania DHCP dla poszczególnych SSID,
4. Weryfikacja poprawności działania założonej polityki bezpieczeństwa dostępu do WLAN we wszystkich SSID zgodnie z założeniami projektowymi,
5. Test działania roamingu L2/L3 – mobilna wędrówka po całym obszarze będącym w zasięgu sieci WLAN i równoczesne wysyłanie standardowych pakietów ping na zewnętrzny adres sieciowy z notebooków testowych asocjowanych w danym SSID.
6. Pomiary jakości wdrożonej sieci:
   a) Pomiar i badanie propagacji fal radiowych w celu określenia zasięgu sieci bezprzewodowej - zakończone raportami pomiary zasięgu sieci WLAN zrealizowane za pomocą profesjonalnego oprogramowania (np. Ekahau lub AirMagnet Survey) dla pasma częstotliwości 2,4 i 5 GHZ. Raporty te powinny jednoznacznie wskazać miejsca o niskim pokryciu sygnałem, które mogę zostać usunięte na dalszym etapie weryfikacji poprzez dodanie nowych AP lub relokację już istniejących,

b) Analiza pokrycia obszaru sygnałem radiowym oraz eliminacja stref z niskim poziomem sygnału radiowego - analiza powyższych raportów, oraz usunięcie obszarów niepokrytych sygnałem WLAN. Po zmianach lokalizacji AP pomiary winny zostać powtórzone. Dopuszczalny najniższy poziom sygnału w zadanych przez Zamawiającego obszarach powinien wynosić minimum - 70dBm dla pasma 2.4GHz oraz - 65dBm dla pasma 5GHz.

c) Analiza widma sygnału radiowego oraz wykrywanie i eliminacja źródeł zakłóceń - weryfikacja i poszukiwanie potencjalnych źródeł zakłóceń i interferencji za pomocą analizatora widma (np. Ekahau Spectrum Analyzer lub AirMagnet Spectrum XT). Pomiary zakończone raportami. Po zlokalizowaniu potencjalnych źródeł interferencji RF - jeżeli nie ma możliwości ich eliminacji (wyłączenie lub przeniesienie zidentyfikowanych urządzeń interferujących), należy przeprojektować sieć w taki sposób, aby zapewnić minimalny poziom parametru SNR (Signal-to-Noise Ratio) na poziomie 25 dB dla pasma 2.4GHz oraz 30dB dla pasma 5GHz.

7. Przygotowanie raportu podsumowującego wyniki testów
8. Ewentualna rekonfiguracja parametrów pracy systemu

4.9. Procedura odbiorowa infrastruktury IT (część dostaw sprzętu i licencji)

Procedura dotyczy odbiorów dokonywanych w zakresie realizacji Przedmiotu Zamówienia, określonych w Harmonogramie wdrożenia. Do Wykonawcy należy przedstawienie w dokumentacji projektowej zakresu odbiorów częściowych, komponentów, etapów zgodnie z SWZ. wraz z przyporządkowaniem terminów i kwot. Dokumentacja projektowa jest częścią analizy przedwdrożeniowej i musi być wykonana i dostarczona w terminach określonych w części dotyczącej analizy przedwdrożeniowej.

4.9.1. Odbiór częściowy

1. Odbiory częściowe (dla robót ulegających zakryciu) dokonywane są w terminach uzgodnionych pomiędzy Zamawiającym i Wykonawcą.
2. Odbiór częściowy potwierdzony jest wpisem do dziennika budowy (jeżeli dotyczy).
3. Jeżeli dziennik budowy nie będzie prowadzony odbiór etapu potwierdzony będzie Protokołem odbioru częściowego podpisanym przez Wykonawcę i Zamawiającego bez zastrzeżeń

4.9.2. Odbiór komponentów

1. Odbiory Komponentów dokonywane są w terminach wskazanych w Harmonogramie wdrożenia.
2. W ramach Odbioru Komponentu, dokonuje się weryfikacji ilościowej, czy w ramach odbieranego Komponentu zostały dostarczone lub wytworzone wszystkie Produkty zgodnie z założeniami określonymi w Harmonogramie wdrożenia.
3. Dokonanie odbioru Komponentu, nie pozbawia Zamawiającego roszczenia wobec Wykonawcy o usunięcie Wad, które ujawnią się w odebranych już Komponentach, w trakcie realizacji kolejnych etapów Umowy, a także w okresie gwarancji.
4. Protokół Odbioru Komponentu, zostanie sporządzony w trzech jednobrzmiących egzemplarzach - dwóch dla Zamawiającego i jednym dla Wykonawcy. Protokół jest dokumentem poświadczającym prawidłowe wykonanie prac.

4.9.3. Odbiór etapu

1. Odbiory etapów dokonywane są w terminach wskazanych w Harmonogramie wdrożenia.
2. W ramach Odbioru etapu dokonuje się weryfikacji ilościowej, czy w ramach odbieranego etapu zostały wytworzone wszystkie Komponenty, zgodnie z założeniami określonymi w DAP.
3. W ramach Odbioru etapu, jeżeli jest to zaplanowane, zostaną przeprowadzone odpowiednie testy funkcjonalne, opisane w Procedurze testowania,
4. Wykonawca przystępując do Odbioru etapu musi przedstawić:
   a) Raport z przeprowadzonych testów funkcjonalnych, przyjęty przez Zamawiającego bez zastrzeżeń (jeżeli były wykonywane w ramach Odbioru etapu),
   b) Raport z doprowadzenia pomieszczeń do stanu nie gorszego niż przed rozpoczęciem robot
   c) Komplet Dokumentacji użytkowej.
   d) Wszystkie Protokoły odbiorów Komponentów wymagane w ramach Odbioru etapu,
   e) oświadczenie kierownika budowy o zgodności wykonania Komponentów w danym etapie Umowy z wymaganiami
   f) oryginał dziennika budowy wraz z wpisem o gotowości do odbioru Komponentów w danym etapie Umowy
5. Odbiór etapu potwierdzony jest Protokołem odbioru etapu podpisanym przez Wykonawcę, Inspektora nadzoru i Zamawiającego bez zastrzeżeń oraz wpisem do dziennika budowy.
6. Jeżeli Protokół odbioru etapu będzie zawierał istotne zastrzeżenia, etap uważa się za nieodebrany.
7. Protokół Odbioru etapu, zostanie sporządzony w trzech jednobrzmiących egzemplarzach - dwóch dla Zamawiającego i jednym dla Wykonawcy.
8. Dokonanie Odbioru etapu, nie pozbawia Zamawiającego roszczenia wobec Wykonawcy o usunięcie wad, które ujawnią się w odebranych już Komponentach wykonanych i dostarczonych w ramach etapu, w trakcie realizacji kolejnych etapów przedmiotu Umowy, a także w okresie gwarancji.
9. Wady Komponentów wykonanych i dostarczonych w ramach konkretnego etapu, zdiagnozowane w etapach późniejszych, zostaną niezwłocznie (jednak nie później niż w terminie wskazanym przez Zamawiającego) usunięte przez Wykonawcę bez odrębnego wynagrodzenia. Zamawiający nie przewiduje, w związku z opisanymi w zdaniach poprzednich okolicznościami, zmiany terminów wykonywania przedmiotu Umowy, w tym kolejnych etapów.

4.9.4. Odbiór końcowy

1. Odbiór końcowy odbędzie się w terminie wskazanym w Harmonogramie wdrożenia.
2. W ramach Odbioru końcowego dokonuje się weryfikacji ilościowej, czy w czasie trwania wdrożenia zostały odebrane wszystkie etapy i zostały wytworzone wszystkie Komponenty, zgodnie z założeniami określonymi w DAP.
3. Wykonawca przystępując do Odbioru końcowego musi przedstawić:
   a) Wszystkie Protokoły odbioru etapów wymagane w ramach Odbioru końcowego,
   b) oświadczenie kierownika budowy o zgodności wykonania Przedmiotu Zamówienia z wymaganiami

c) oryginał dziennika budowy wraz z wpisem o gotowości do Odbioru końcowego
d) Komplet Dokumentacji,
e) Potwierdzenie usunięcia wszystkich wad ujawnionych po Odbiorach Komponentów i Odbiorach etapów.
f) Spis wszystkich loginów i haseł dostępu do wszystkich urządzeń.

4. Odbiór końcowy potwierdzony jest Protokołem odbioru końcowego podpisanym przez Wykonawcę, Zamawiającego i Inspektora nadzoru bez zastrzeżeń Protokół zostanie sporządzony w trzech jednobrzmiących egzemplarzach - 2 dla Zamawiającego, 1 dla Wykonawcy stanowi podstawę do wystawienia faktury VAT na zasadach określonych w Umowie.

4.10. Szkolenia

Wykonawca jest zobowiązany do przeszkolenia wszystkich użytkowników systemów zainstalowanych w pełnym zakresie obsługi i administracji, dla użytkownika i administratora. Podczas szkolenia użytkowników musi zostać przekazana niezbędna wiedza w zakresie poprawnego użytkowania wrażanych systemów w obrębie poszczególnych modułów w zakresie funkcjonowania, obsługi, administrowania i utrzymania systemów.

1. Zakres szkoleń musi obejmować praktyczną obsługę wszystkich funkcjonalności systemów.
2. Szkolenia muszą być prowadzone przez wykwalifikowanych specjalistów Wykonawcy, posiadających niezbędną wiedzę fachową w zakresie tematyki szkoleń.
3. Szkolenia będą musiały być przeprowadzane w siedzibie Zamawiającego, na dokumentach i sprzęcie Zamawiającego.
4. Wykonawca zapewni realizację szkoleń użytkowników w wymiarze niezbędnym do przyswojenia wiedzy z pełnego zakresu wdrożenia.
5. Wykonawca pokryje wszelkie koszty związane z przeprowadzeniem szkoleń.
6. Każda z osób biorących udział w szkoleniu musi mieć dostęp do stacji roboczej.
7. Długość szkoleń należy określić z administratorem.
8. Szkolenia mogą się odbyć po terminie odbioru, w takim wypadku wykonawca musi przekazać voucher na szkolenie w akredytowanej jednostce lub u siebie z terminem wykonania nie dłuższym niż pół roku ale nie krótszym niż 3 miesiące.

4.11. Obsługa serwisowa

1. Przedmiotem Zamówienia jest sprawowanie przez Wykonawcę obsługi serwisowej oraz bieżącego nadzoru nad Sprzętem, przez okres 3 lat po podpisaniu protokołu odbioru, co w szczególności oznacza:
   a) przygotowywanie Aktualizacji (Upgrade'ów) w zakresie objętym nadzorem nad infrastrukturą i urządzeniami nie rzadziej niż raz na miesiąc. Wykonawca rozpocznie prace mające na celu przygotowanie Aktualizacji (Upgrade'u) nie później niż w dniu opublikowania odpowiednich przepisów prawnych lub oprawek i wykona je tak aby termin instalacji Aktualizacji (Upgrade'u) Systemu pozwalał na jej zastosowanie zgodnie z terminem wejścia w życie

zmienionych lub nowych przepisów (w przypadku, gdyby termin opublikowania przepisów prawnych nie pozwalał na przygotowanie Aktualizacji (Upgrade'u) w tym terminie, Strony uzgodnią inny termin wprowadzenia zmian z uwzględnieniem możliwości realizacji w jak najkrótszym czasie);

b) udostępnienie i zainstalowanie przez Wykonawcę Aktualizacji (Upgrade'ów) i Poprawek (Update'ów) bez obowiązku ponoszenia dodatkowych opłat z tego tytułu przez Zamawiającego;
c) udzielanie konsultacji telefonicznych za pośrednictwem wydzielonych linii telefonicznych „helpdesk" w dni robocze w godzinach 8.00-16:00 w celu:
    1. pomocy w przypadku trudności w wykonaniu prac operatorskich;
    2. pomocy w diagnostyce problemów związanych z działaniem infrastruktury;
d) przyjmowanie zgłoszeń Błędów blokujących, Błędów krytycznych oraz Usterek za pośrednictwem Systemu Obsługi Zgłoszeń w trybie 24 godziny przez 7 dni w tygodniu. Błędy blokujące prace będą dodatkowo zgłaszane w godzinach 16: 00 – 08: 00 na dyżurny numer „helpdesk";
e) usuwanie zgłoszonych przez Zamawiającego Błędów krytycznych oraz Usterek, ujawnionych w trakcie eksploatacji Systemu;
f) diagnostyka, optymalizacja i serwis działania infrastruktury;
g) podejmowanie działań wyprzedzających w odpowiedzi na zgłoszenia z automatów monitorujących parametry krytyczne Systemu (monit) w zakresie nieprawidłowego działania infrastruktury;
h) informowanie Zamawiającego i Zarządcę o nowych aktualizacjach Systemu;
i) udostępnianie Zamawiającemu wraz z nowymi wersjami Systemu (Aktualizacjami) dokumentacji technicznej

2. Wykonawca oświadcza, że ma prawo do wykonywania usług związanych z Systemem będących przedmiotem niniejszego opisu oraz zobowiązuje się realizować serwis z zachowaniem należytej staranności, zgodnie ze swoją wiedzą oraz z wykorzystaniem wysoko wykwalifikowanego i doświadczonego zespołu specjalistów w zakresie przedmiotu Umowy, posiadającego wymagane doświadczenie w wykonywaniu prac odpowiadających swoim zakresem zakresowi niniejszej Umowy.
3. Zamawiający ma prawo do zmian w konfiguracji urządzeń i infrastruktury zgodnie ze sztuką co nie spowoduje zmian w zakresie gwarancji.
4. Terminy usuwania wad znajdują się w Umowie.
5. Wykonawca musi uruchomić automatyczny portal internetowy – portal zgłoszeniowy.

5.Część Informacyjna PFU

Dokumenty potwierdzające zgodność zamierzenia budowlanego z wymaganiami wynikającymi z odrębnych przepisów

Wykonawca uzyska niezbędne decyzje administracyjne (jeżeli wymagane) związane z wykonaniem przedmiotu zamówienia własnym kosztem i staraniem. Wszelkie niezbędne dokumenty Wykonawca przedłoży Zamawiającemu do akceptacji i podpisu. Zamawiający udzieli pełnomocnictw Wykonawcy, z którym zostanie zawarta umowa

Oświadczenie Zamawiającego stwierdzające jego prawo do dysponowania nieruchomością na cele budowlane

Zamawiający oświadcza, że posiada stosowne prawo do dysponowania nieruchomościami na potrzeby przeprowadzenia prac objętych niniejszym PFU.

Przepisy prawne i normy związane z projektowaniem i wykonaniem zamierzenia budowlanego

Dokumentacja Projektowa oraz przeprowadzone prace muszą spełniać obowiązujące przepisy Prawa Budowlanego, przepisy techniczno-budowlane, przepisy związane i obowiązujące poniższe normy lub rozwiązania równoważne:

Rozporządzenia Ministra Infrastruktury w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego.
Rozporządzenie (WE) Parlamentu Europejskiego i Rady nr 2195/2002 z dnia 5 listopada 2002 roku w sprawie Wspólnego Słownika Zamówień.
Rozporządzenie Ministra Infrastruktury z dnia 18 maja 2004 roku w sprawie określenia metod i podstaw sporządzenia kosztorysu inwestorskiego, obliczania planowanych kosztów prac projektowych oraz planowanych kosztów robót budowlanych określonych w programie funkcjonalno-użytkowym.
Ustawa Prawo Budowlane oraz wydanych na jej podstawie rozporządzeń.
Ustawa z dnia 30 sierpnia 2002 roku o systemie oceny zgodności.
Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego.
Rozporządzenie Ministra Pracy i Polityki Socjalnej z 1 grudnia 1998 roku w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory.
Ustawa z 16 lipca 2004 roku Prawo Telekomunikacyjne.
Ustawa z dnia 30 maja 2014 r. o prawach konsumenta.
Ustawa z dnia 29 stycznia 2004 roku Prawo Zamówień Publicznych.
Rozporządzenie Ministra Infrastruktury z dnia 23 czerwca 2003 roku w sprawie informacji dotyczącej zdrowia oraz planu bezpieczeństwa i ochrony zdrowia.
Rozporządzenie Ministra Infrastruktury z dnia 6 lutego 2003 roku w sprawie bezpieczeństwa i higieny pracy podczas wykonywania robót budowlanych.
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 24 lipca 2009 roku w sprawie przeciwpożarowego zaopatrzenia w wodę oraz dróg pożarowych.
Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 roku w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy.

Normy europejskie - oznaczają normy przyjęte prze Europejski Komitet Standaryzacji (CEN) oraz Europejski Komitet Standaryzacji Elektrotechnicznej (CENELEC) jako „Standardy europejskie (EN) ” lub dokumenty „harmonizacyjne (HD)” zgodnie z ogólnymi zasadami działania tych organizacji.
Warunki techniczne wykonania i odbioru robót budowlano-montażowych (część I Roboty ogólnobudowlane ITB, wyd. II).
Warunki techniczne wykonywania i odbioru robót budowlano-montażowych. Instalacje elektryczne. Wydawnictwo "Arkady" 1990.
PN-IEC 60364:2000 Instalacje elektryczne w obiektach budowlanych.
PN-EN 50174-1: 2002 Technika informatyczna. Instalacja okablowania. Specyfikacja i zapewnienie jakości.
PN-EN 55022: 2002 Kompatybilność elektromagnetyczna. Dopuszczalny poziom i metody zakłóceń radioelektrycznych wytwarzanych przez urządzenia informatyczne.
PN-EN 50082-1: 2002 Kompatybilność elektromagnetyczna. Wymagania ogólne dotyczące odporności na zaburzenia.
PN-EN 50081-2: 2002 Kompatybilność elektromagnetyczna. Wymagania ogólne dotyczące emisyjności.
PN-EN 50310:2016 Sieci połączeń wyrównawczych w budynkach i innych obiektach budowlanych z instalacjami telekomunikacyjnymi.
PN-EN 50364: 2003 Technika informatyczna. Instalacja okablowania. Testowanie zainstalowanego okablowania.
PN-79/T-052 10: 1979 Antenowe instalacje zbiorowe. Ogólne wymagania i badania.
BN-8984-05 Kanalizacja kablowa. Ogólne badania i wymagania.
PN-T-01003 Słownictwo telekomunikacyjne. Telefonia. Nazwy i określenia.
PN-T-06700 Bezpieczeństwo pracy przy promieniu emitowanym przez urządzenia laserowe. Klasyfikacja sprzętu. Wymagania i wytyczne dla użytkownika.
BN-3233-13 Telekomunikacyjne linie kablowe. Opaski oznaczeniowe.
BN-6353-03 Folia kalandrowana techniczna z uplastycznionego polichlorku winylu.
ZN-TP S.A.-002 Telekomunikacyjne linie kablowe dalekosiężne. Linie optotelekomunikacyjne. Ogólne wymagania techniczne.
ZN-TP S.A.-005 Kable optotelekomunikacyjne. Wymagania i badania.
N-TP S.A.-007 Złączki światłowodowe i kable stacyjne. Wymagania i badania.
ZN-TP S.A.-008 Osłony złączowe. Wymagania i badania.
ZN-TP S.A.-011 Telekomunikacyjna kanalizacja kablowa. Ogólne wymagania techniczne.
ZN-TP S.A.-012 Kanalizacja pierwotna. Wymagania i badania.
ZN-TP S.A.-025 Taśmy ostrzegawczo-lokalizacyjne. Wymagania i badania.
WTE-ZDBŁ-22 Wymagania techniczno - eksploatacyjne na kable optotelekomunikacyjne jednomodowe, ZDBŁ, Warszawa.
Instrukcja TP S.A. T-01. Odbiór i utrzymanie kablowych linii optotelekomunikacyjnych.
DT-ZDBŁ-43 Pomiar tłumienności, lokalizacja niejednorodności i uszkodzeń telekomunikacyjnych kabli światłowodowych reflektometrem, ZDBŁ, Warszawa.

DT-ZDBŁ-45 Wstępna technologia wykonywania złączy kabli światłowodowych z wykorzystaniem mufy MS. CzDDrjZDBŁ, Warszawa.
DT-ZDBŁ-47 jak wyżej, CzD DD, ZDBŁ, Warszawa.
DT-ZDBŁ-51 jak wyżej, CzD DII, ZDBŁ, Warszawa.
DT-ZDBŁ-57 Technologia pneumatycznego zaciągania (z wpychaniem) kabli światłowodowych do kanalizacji, ZDBŁ, Warszawa.
IT-ZDBŁ-52 Wstępna instrukcja zacinania kabli światłowodowych do kanalizacji kablowej oraz budowy kanalizacji wtórnej, ZDBŁ, Warszawa.
IT-ZDBŁ-55 Wstępna instrukcja układania kabli światłowodowych w ziemi i w wodzie, ZDBŁ, Warszawa.
IT-ZDBŁ-60 Instrukcja układania kabli światłowodowych kanałowych, ZDBŁ.
Załącznik do Zarządzenia nr 83 Dyrektora Pionu Sieci Tadeusza Gracy z dnia 12 maja 2003 r – Instrukcja oznaczenia elementów stosowanych w sieci telekomunikacyjnej TP SA.
ISO/IEC 11801 Information technology. Generic cabling for customer premises.
EN 50173-1 Information technology. Generic cabling systems Part 1: "General requirements".
ANSI/TIA/EIA 568-B.2 Commericial Building Telecommunications Cabling Standards Part 2".
PN-EN 50173-1:2011 Technika informatyczna. Systemy okablowania strukturalnego. Część 1: Wymagania ogólne.
PN-EN 50173-2: 2008/A1:2010 Technika informatyczna. Systemy okablowania strukturalnego. Część 2: Pomieszczenia biurowe.
PN-EN 50173-1 Technika informatyczna. Systemy okablowania strukturalnego. Część 1: Wymagania ogólne.
PN-EN 50173-5:2009/A1:2011+A2:2013 Technika informatyczna. Systemy okablowania strukturalnego. Część 5: Centra danych.
PN-EN 50173-6:2014 Technika informatyczna. Systemy okablowania strukturalnego. Część 6: Rozproszone usługi budynkowe.
PN-EN 50174-1:2010/A1:2011+A2:2015 Technika informatyczna. Instalacja okablowania – Część 1- Specyfikacja i zapewnienie jakości.
PN-EN 50174-2:2010/A1:2011+A2:2015 Technika informatyczna. Instalacja okablowania – Część 2 - Planowanie i wykonawstwo instalacji wewnątrz budynków.
PN-EN 50174-3:2014 Technika informatyczna. Instalacja okablowania – Część 3 – Planowanie i wykonawstwo instalacji na zewnątrz budynków.
PN-EN 50575:2015 Kable i przewody elektroenergetyczne, sterownicze i telekomunikacyjne -- Kable i przewody do zastosowań ogólnych w obiektach budowlanych o określonej klasie odporności pożarowej.
IEC 61935-1:2015 Specification for the testing of balanced and coaxial information technology cabling - Part 1: Installed balanced cabling as specified in ISO/IEC 11801 and related standards.
ISO/IEC 14763-3:2014 Implementation and operation of customer premises cabling - Part 3: Testing of optical fibre cabling.
ISO/IEC TS 29125:2017 Information technology -- Telecommunications cabling requirements for remote powering of terminal equipment.

ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) 2016/364 z dnia 1 lipca 2015 r. w sprawie klasyfikacji reakcji na ogień wyrobów budowlanych na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 305/2011.

Inne posiadane informacje i dokumenty niezbędne do zaprojektowania robót budowlanych

Inne posiadane informacje i dokumenty niezbędne do zaprojektowania robót budowlanych:

Kopia mapy zasadniczej

Wykonawca przed przystąpieniem do prac projektowych we własnym zakresie uzyska aktualną mapę do celów projektowych dla rozbudowy, przebudowy lub udrożnienia kanalizacji teletechnicznej, jeśli roboty te będą wymagały takiej mapy.

Wyniki badań gruntowo-wodnych na terenie budowy dla potrzeb posadowienia obiektów

Nie dotyczy.

Zalecenia konserwatorskie konserwatora zabytków

Zakres projektu nie dotyczy pomieszczeń lub budynków objętych ochroną Wojewódzkiego Konserwatora Zabytków.

Inwentaryzacja zieleni

O ile wystąpi taka potrzeba przy ewentualnej rozbudowie, przebudowie lub udrażnianiu kanalizacji teletechnicznej wykonanie inwentaryzacji zieleni leży po stronie Wykonawcy.

Dokumenty z zakresu ochrony środowiska

Dane dotyczące zanieczyszczeń atmosfery do analizy ochrony powietrza oraz posiadane raporty, opinie lub ekspertyzy z zakresu ochrony środowiska – nie dotyczy.

Wykonawca przed przystąpieniem do prac projektowych we własnym zakresie uzyska dokumenty z zakresu ochrony środowiska, niezbędnych badań, raportów, ekspertyz dla rozbudowy, przebudowy lub udrożnienia kanalizacji teletechnicznej, jeśli roboty te będą wymagały takich dokumentów.

Pomiary ruchu drogowego, hałasu i innych uciążliwości

Nie dotyczy.

Inwentaryzacja lub dokumentacja obiektów budowlanych

Wykonawca we własnym zakresie dokona inwentaryzacji architektonicznej obiektu objętego niniejszym PFU. Dodatkowo Wykonawca zinwentaryzuje instalacje i urządzenia technologiczne podlegające rozbudowie.

Dokumenty związane z przyłączami

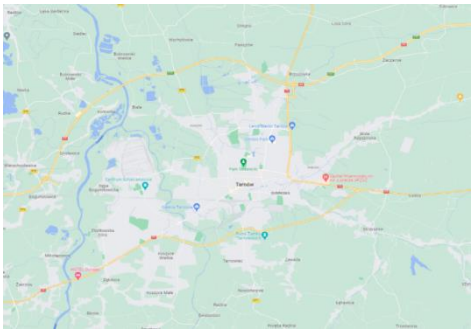
Porozumienia, zgody lub pozwolenia oraz warunki techniczne i realizacyjne związane z przyłączem telekomunikacyjnym o ile będzie to konieczne należy uzyskać w imieniu Zamawiającego. Zamawiający w takim przypadku przekaże stosowne pełnomocnictwa.

Porozumienia, zgody lub pozwolenia oraz warunki techniczne i realizacyjne związane z przyłączeniem obiektu do istniejących sieci wodociągowych, kanalizacyjnych, cieplnych, gazowych, energetycznych oraz dróg samochodowych, kolejowych lub wodnych - nie dotyczy.

Dodatkowe wytyczne inwestorskie i uwarunkowania związane z budową i jej przeprowadzeniem

Roboty budowlane będą prowadzone w czynnym obiekcie użyteczności publicznej. Wykonawca ma obowiązek zabezpieczenia terenu budowy – frontu robót i znajdującego się na nim mienia, swoim kosztem i staraniem do czasu ostatecznego zakończenia robót i ich protokolarnego odbioru przez Zamawiającego. Roboty będą zorganizowane w sposób umożliwiający wykonywanie funkcji Zamawiającego, zapewniający bezpieczeństwo osób zatrudnionych oraz przebywających w obiektach. Godziny robót oraz sposób korzystania z mediów (gaz, co, cwu, energia elektryczna, etc.) Wykonawca będzie uzgadniał z Zamawiającym przed rozpoczęciem robót.

Położenie obiektów



Wzory raportów

1. Wzór raportu z testów
2. Wzór protokołu odbioru

ZAŁĄCZNIK NR 1 DO PFU

WZÓR RAPORTU Z TESTÓW
z dnia ../../..

Umowa i numer	*Umowa nr ..*

sporządzony w dniu ../../.. w ..

PARAMETR	ZAMAWIAJĄCY	WYKONAWCA
Nazwa	..	..
Adres	..	..
Data odbioru	../../..	
Osoby biorące udział w testach	..	..

Lp	SPECYFIKACJA i ZAKRES TESTÓW	WYNIKI *[pozytywne / negatywne]*	AKCEPTACJA WYNIKÓW *[Akceptacja / Brak akceptacji]*	UWAGI / ZASTRZEŻENIA	TERMIN USUNIĘCIA UWAG / ZASTRZEŻEŃ
1)	..	..	..	..	..

PODPIS OSÓB UPRAWNIONYCH

Data podpisania raportu: ../../..

Zamawiający: Wykonawca:

WZÓR PROTOKOŁU ODBIORU
z dnia ../../..

Umowa i numer	*Umowa nr ..*

sporządzony w dniu ../../.. w ..

PARAMETR	ZAMAWIAJĄCY	WYKONAWCA
Nazwa	..	..
Adres	..	..
Data odbioru	../../..	
Osoby uprawnione do przeprowadzenia czynności odbioru	..	..

Lp	SPECYFIKACJA ZREALIZOWANYCH PRAC	Ilość
2)	..	..

Lp.	LISTA UWAG/ZASTRZEŻEŃ
1)	..

PODPIS OSÓB UPRAWNIONYCH

Data podpisania protokołu: ../../..

Zamawiający: Wykonawca: