

**Dokumentacja projektowa instalacji okablowania  
strukturalnego z urządzeniami aktywnymi**

Przedmiot opracowania:

Projekt sieci LAN i zasilania dedykowanego w UMiG Proszowice.

Inwestor:

Urząd Gminy i Miasta przy ul. 3 Maja 72 w Proszowicach

Adres obiektu:   Urząd Gminy i Miasta w Proszowicach  
                            ul. 3 Maja 72, 32-100 Proszowice

Projekt wykonawczy, branża teletechniczna

	Imię i nazwisko	Data	Podpis
Projektował:	Janusz Wojdyła 0349/97/U	07.2019	
Sprawdził:	Eugeniusz Chuderski 1628/99/U	07.2019	

**Kraków, lipiec 2019 r.**

## Spis treści

1	Spis rysunków.....	4
2	Zakres projektu .....	5
3	Podstawa opracowania projektu .....	5
4	Wymagania ogólne dotyczące systemu okablowania strukturalnego .....	5
5	Wymagania szczegółowe dotyczące systemu okablowania strukturalnego .....	6
5.1	Trasy kablowe .....	7
5.1.1	Prowadzenie okablowania.....	7
5.1.2	Separacja okablowania poziomego od kabli elektrycznych .....	7
5.1.3	Prowadzenie kabli w pionach kablowych .....	7
5.1.4	Trasy kablowe wewnątrz pomieszczeń punktów dystrybucyjnych .....	7
5.2	Okablowanie poziome .....	7
5.2.1	Wymagania dla Punktu Logicznego (PL) .....	7
5.2.2	Wymagania dla kabli symetrycznych .....	9
5.2.3	Wymagania dla modułów gniazd RJ45.....	9
5.2.4	Wymagania dla wtyków RJ45 (MPTL - zastosowanie opcjonalne) .....	10
5.2.5	Wymagania dla paneli krosowych okablowania symetrycznego .....	11
5.2.6	Wymagania dla kabli krosowych miedzianych / strona szafy .....	12
5.2.7	Wymagania dla kabli dołączeniowych / strona użytkownika.....	12
5.3	Okablowanie szkieletowe .....	13
5.3.1	Wymagania dla kabla światłowodowego wielomodowego .....	13
5.3.2	Wymagania dla obudowy światłowodowej.....	14
5.3.3	Wymagania dla kaset światłowodowych .....	15
5.3.4	Wymagania dla tac na spawy światłowodowe .....	15
5.3.5	Wymagania dla pigtaili światłowodowych LC OM3.....	15
5.3.6	Wymagania dla kabli krosowych światłowodowych OM3 .....	15
5.4	Urządzenia aktywne .....	16
5.4.1	Założenia ogólne: .....	16
5.4.2	Wymagania szczegółowe dla systemów zarządzania i monitorowania infrastrukturą siecią i dostępem do sieci LAN i WLAN.....	17
5.4.3	Wymagania szczegółowe dla systemu zarządzania siecią .....	19
5.4.4	Wymagania szczegółowe dla kompleksowego systemu kontroli dostępu do sieci .....	22
5.4.5	Wymagania szczegółowe dla poszczególnych komponentów sieciowych .....	25
5.4.6	Wymagania szczegółowe dla urządzeń typu Przełącznik dostępowy 48 portowy POE+ .....	28
5.4.7	Wymagania szczegółowe dla urządzeń typu Przełącznik dostępowy 48 portowy POE+ z portami 10Gb.....	29

5.4.8	Wymagania szczegółowe dla urządzeń typu Przełącznik dostępowy 24 portowy z PoE+ .....	29
5.4.9	Wymagania szczegółowe dla urządzeń typu Przełącznik 12 portowy .....	30
5.4.10	Wymagania szczegółowe dla urządzeń Punkt dostępowy .....	30
5.5	Punkty dystrybucji okablowania strukturalnego .....	31
5.5.1	Szafy dystrybucyjne .....	31
5.5.2	Listwy zasilające PDU .....	32
5.5.3	Organizery poziome .....	34
5.5.4	Organizery pionowe .....	34
6	Administracja .....	34
7	Gwarancja oraz wymagania dotyczące kompetencji .....	34
7.1	Obowiązki producenta okablowania .....	34
7.2	Obowiązki instalatora .....	35
8	Odbiór i pomiary sieci okablowania strukturalnego .....	35
8.1	Pomiary okablowania miedzianego .....	36
8.2	Pomiary okablowania światłowodowego .....	36
8.3	Zawartość dokumentacji powykonawczej .....	36
9	Oświadczenie projektanta i sprawdzającego .....	38
10	Uprawnienia .....	39
11	Rysunki .....	43

## 1 Spis rysunków

L.P	Tytuł rysunku	Nr Rys.
1	Rzut piwnicy - teletechnika	<b>T-01</b>
2	Rzut parteru – teletechnika	<b>T-02</b>
3	Rzut I piętra - teletechnika	<b>T-03</b>
4	Schemat ideowy sieci LAN	<b>T-04</b>
5	Schemat ideowy szaf GPD	<b>T-05</b>
6	Schemat ideowy szafy PPD	<b>T-06</b>
7		
8		
9		
10		
11		
12		
13		

## 2 Zakres projektu

Przedmiotem niniejszego opracowania jest projekt kompleksowej instalacji sieci LAN obejmujący część pasywną oraz aktywną. Projekt wykonywany ma być dla Urzędu Miasta i Gminy w Proszowicach i opracowany na podstawie uzgodnień z Inwestorem oraz wszystkich niniejszych wytycznych przy uwzględnieniu funkcjonalności systemu oraz wymagań dla nowoczesnych urządzeń transmisji danych.

Wytyczne opisują minimalne wymagania Inwestora w zakresie technicznym i funkcjonalnym. Oznacza to, że można zastosować rozwiązania spełniające wszystkie kryteria opisane w dokumentacji projektowej, tj. zgodne pod kątem obowiązującej normalizacji, wymaganych parametrów oraz funkcji. **Składając ofertę, wykonawca ma przedstawić nazwę producenta oraz listę materiałów w formie tabeli, zawierającej numery katalogowe, nazwy produktów oraz ilości.**

## 3 Podstawa opracowania projektu

Podstawą do opracowania projektu okablowania strukturalnego są wymagania Inwestora w zakresie funkcjonalności i wydajności systemu oraz obowiązujące normy.

Lista norm wykorzystanych w projekcie:

**PN-EN 50173-1:2018-07**

Technika Informatyczna – Systemy okablowania strukturalnego – Część 1: Wymagania ogólne;

**PN-EN 50173-2:2018-07**

Technika Informatyczna – Systemy okablowania strukturalnego – Część 2: Budynki biurowe;

**PN-EN 50173-5:2018-07**

Technika Informatyczna – Systemy okablowania strukturalnego – Część 2: Centra danych;

**PN-EN 50173-6:2018-07**

Technika Informatyczna – Systemy okablowania strukturalnego – Część 6: Rozproszone usługi budynkowe;

**PN-EN 50174-1:2018-08**

Technika informatyczna. Instalacja okablowania – Część 1- Specyfikacja instalacji i zapewnienie jakości;

**PN-EN 50174-2:2018-08**

Technika informatyczna. Instalacja okablowania – Część 2 - Planowanie i wykonawstwo instalacji wewnątrz budynków;

**PN-EN 50174-3:2014-02/A1:2017-07**

Technika informatyczna. Instalacja okablowania – Część 3 – Planowanie i wykonawstwo instalacji na zewnątrz budynków;

**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/Amd1:2018**

Implementation and operation of customer premises cabling - Part 3: Testing of optical fibre cabling;

Wykonawca ma obowiązek wykonać instalację okablowania zgodnie z wymaganiami opisanymi w niniejszej specyfikacji oraz powołanymi i powiązanymi z nimi normami a także zastosować się obligatoryjnie do wszelkich wymagań producenta stosowanego systemu okablowania strukturalnego w celu objęcia go po instalacji gwarancją systemową na okres min. 25 lat.

Jeśli którykolwiek z dokumentów normalizacyjnych uległ aktualizacji w stosunku do wymienionych powyżej, według nowych aktualnych wymagań.

## 4 Wymagania ogólne dotyczące systemu okablowania strukturalnego

- Rozmieszczenie stanowisk roboczych przyjąć na podstawie ustaleń z Użytkownikiem oraz najbardziej aktualnej aranżacji wnętrz dla pomieszczeń na etapie realizacji inwestycji;
- Piętrowy Punkt Dystrybucyjny (PPD) należy zlokalizować w pomieszczeniu nr. 13 (pok.49) na I piętrze zapewniając odpowiednią przestrzeń min. 1000mm z przodu;

- Główny Punkt Dystrybucyjny (GPD) zostanie zlokalizowany w pomieszczeniu serwerowni nr 28 w piwnicy;
- Osłony zewnętrzne kabli miedzianych i światłowodowych mają być trudnopalne i niewydzielające trujących substancji w obecności ognia (LSZH) oraz charakteryzować się Euroklasą min. **Dca-s2a,d2,a1**;
- Punkt PPD należy połączyć z GPD łączami szkieletowymi w następującej konfiguracji:
  - 1 kabel światłowodowy wielomodowy 12xOM3 zakończony złączami LC duplex;
  - 4x kabel F/FTP kategoria 6A;
- Na całość zainstalowanego okablowania ma być udzielona gwarancja bezpośrednio przez producenta na okres minimum 25 lat (szczegółowy opis zawarty w dziale Gwarancja oraz wymagania dotyczące kompetencji);
- Montaż gniazd okablowania poziomego PL ma być realizowany natynkowo przy zastosowaniu płyt czołowych z uchwytyami w standardzie montażowym 45x45;
- Okablowanie poziome ma być prowadzone kablem typu F/FTP spełniającym wymogi minimum kat.6A z pozytywnym pasmem przenoszenia do 500 MHz;
- Okablowanie ma być realizowane poprzez ekranowane moduły gniazd RJ45 kat.6A, dwuelementowe, zarabiane narzędziowo;
- Należy zastosować proste modularne panele krosowe o wysokości 1U na 48 i 24 oddzielne moduły;
- Wszystkie kable okablowania poziomego mają być zakończone w osprzęcie połączeniowym zgodnie z normą PN-EN 50173-1;
- W celu podniesienia bezpieczeństwa użytkowania okablowania, przy zachowanym standardzie złącza RJ45, należy uwzględnić zastosowanie mechanicznych zabezpieczeń - gniazda dostępne dla osób niepowołanych powinny umożliwiać ich zaślepienie zabezpieczając przed niepowołanym podłączeniem się do sieci. O ich udostępnieniu osobie trzeciej powinien decydować administrator sieci zdejmując za pomocą specjalnego klucza blokadę – zaślepkę gniazda.
- Aby zagwarantować i potwierdzić wymaganą wydajność okablowania miedzianego przeznaczonych do zabudowy (kabel oraz gniazdo) producent musi posiadać certyfikaty wydane przez akredytowane niezależne laboratoria (np. ETL, GHMT, Delta) potwierdzające zgodność systemu/komponentów z wymaganiami normy międzynarodowej, tj. ISO/IEC 11801 lub EN50173-1;
- Wszystkie złącza światłowodowe muszą być wypolerowane w fabrycznym procesie produkcyjnym;
- Dla każdego podsystemu (LAN ( z PoE i bez PoE), WLAN, CCTV należy stosować kable krosowe oraz moduły gniazd RJ45 w odpowiednim kolorze dla łatwej identyfikacji i zarządzania systemem – tym samym nie dopuszcza się stosowania rozwiązań które wykorzystują oznaczenia kolorystyczne w formie dodatkowych naklejek/ikon itp. jako oznaczenia nietrwałe;
- Wszystkie miedziane kable krosowe muszą pochodzić od tego samego producenta co reszta komponentów okablowania strukturalnego oraz posiadać deklarację zgodności CE;
- Wszystkie miedziane wtyki kablowe stosowane w połączeniach MPTL muszą pochodzić od tego samego producenta co reszta komponentów okablowania strukturalnego oraz posiadać deklarację zgodności CE;
- W szafach stojących mają być zastosowane wieszaki poziome i pionowe ułatwiające prowadzenie i układanie kabli oraz zarządzanie kablami krosowymi;
- Producent proponowanego systemu okablowania strukturalnego musi posiadać od przynajmniej 7 lat aktualne certyfikaty ISO 9001 i ISO 14001;

## 5 Wymagania szczegółowe dotyczące systemu okablowania strukturalnego

Środowisko wewnątrz budynku, w których będzie instalowany osprzęt kablowy, jest środowiskiem biurowym i zostało ono sklasyfikowane jako M<sub>1</sub>I<sub>1</sub>C<sub>1</sub>E<sub>2</sub> zgodnie z PN-EN 50173-1.

Maksymalne długości kanałów transmisyjnych okablowania poziomego zostały obliczone dla przypadku wzrostu temperatury otoczenia do 40°C.

## **5.1 Trasy kablowe**

### **5.1.1 Prowadzenie okablowania**

Okablowanie ma zostać rozprowadzone:

- na głównych ciągach komunikacyjnych w korytach kablowych należy zabezpieczyć przynajmniej 20% rezerwy na rozbudowę okablowania w przyszłości,
- w pomieszczeniach do punktu logicznego – w korytach kablowych,

### **5.1.2 Separacja okablowania poziomego od kabli elektrycznych**

Kable okablowania strukturalnego oraz elektrycznego, zgodnie z wymogami norm, należy prowadzić w oddzielnych trasach kablowych przy zachowaniu minimalnej separacji wynoszącej 20mm lub zastosowania przegrody.

### **5.1.3 Prowadzenie kabli w pionach kablowych**

Trasy kablowe pionowe mają być zbudowane z drabinek kablowych w wydzielonych szachtach dla instalacji teleinformatycznych. Na każdej kondygnacji należy zainstalować drzwiczki rewizyjne przy szachcie kablowym przy podłodze i suficie. Miejsca przejścia przez stropy są zaznaczone na rzutach. Kable w pionach muszą zostać przytwierdzone do drabinek kablowych przy pomocy miękkich opasek Velcro min. co 30 cm.

### **5.1.4 Trasy kablowe wewnątrz pomieszczeń punktów dystrybucyjnych**

W pomieszczeniach punktów dystrybucyjnych zgodnie z rzutami należy zainstalować przy suficie koryta siatkowe. Koryta doprowadzić nad dachy szaf dystrybucyjnych. Kable wprowadzić do szaf poprzez dach w bocznych obszarach poprzez specjalnie przygotowane do tego otwory nie wchodząc w przestrzeń sprzętu aktywnego co znacznie utrudniłoby jego chłodzenie.

## **5.2 Okablowanie poziome**

Kable okablowania poziomego mają być zakończone w zestawach gniazd, zwanych dalej punktami logicznymi (PL). Gniazda w zestawach (punktach logicznych) występują w różnej ilości i konfiguracji w zależności od lokalizacji i przeznaczenia.

Zestawy gniazd PL mają być zgodne ze standardem uchwytu osprzętu elektroinstalacyjnego typu 45x45mm. Należy zastosować płyty czołowe skośne i ramki wielokrotne.

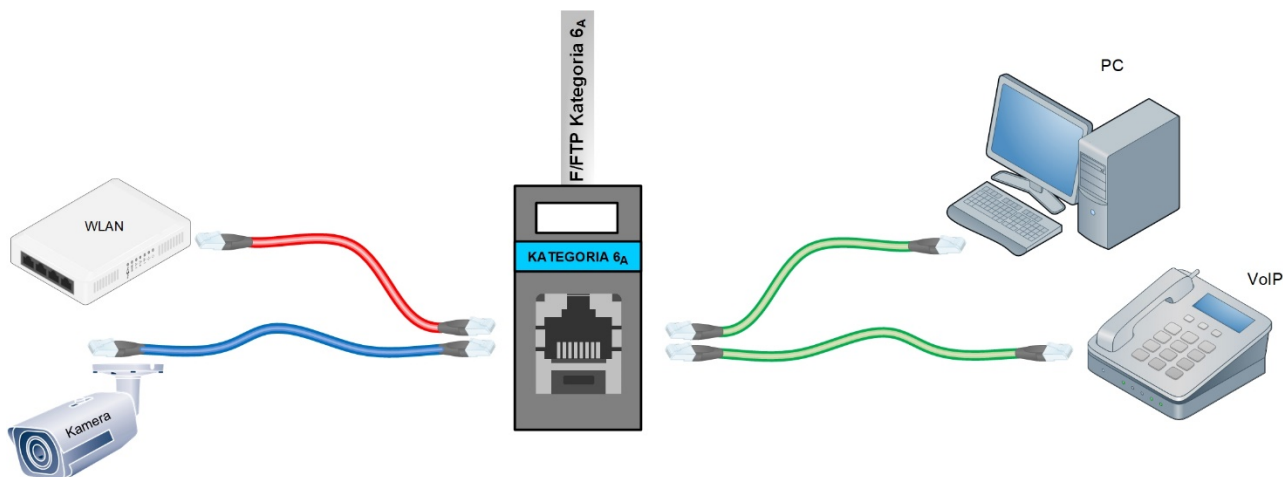
Gniazda sieci elektrycznej dedykowanej należy wykonać zgodnie z projektem zasilania.

### **5.2.1 Wymagania dla Punktu Logicznego (PL)**

Rozmieszczenie stanowisk roboczych przyjąć na podstawie ustaleń z Użytkownikiem oraz najbardziej aktualnej aranżacji wnętrza dla pomieszczeń na etapie realizacji inwestycji;

Do PL doprowadzić kabel symetryczny F/FTP kat.6A. Kable należy zakończyć w gniazdach RJ45 kat.6A lub wtykiem RJ45 kat.6A w zależności od przeznaczenia.

Wszystkie PL ogólnego przeznaczenia należy zakończyć gniazdami RJ45 wg. poniższego schematu.



Rysunek 1. Budowa punktu logicznego PL z gniazdem RJ45

W związku z dużym zagęszczeniem punktów logicznych oraz mocnym zróżnicowaniem tych elementów jeżeli chodzi o podłączone urządzenia przyjęto jednoznaczne przyporządkowanie kolorystyczne modułów RJ45 w gniazdach i panelach krosowych. Rozwiązanie takie zapewnia administratorowi sieci łatwą i szybką orientację od strony szafy kablowej a pracownikom użytkującym sieć nie pozwala na pomyłki związane z wpinaniem się do sieci w nieodpowiedni port. Przyjęta kolorystyka ma swoje odzwierciedlenie w rysunkach szaf kablowych.

Kolor gniazda i kabla krosowego	Przeznaczenie
Zielony	<b>Ogólne bez funkcji PoE+</b> <u>strona panelu krosowego</u> - moduł ma być wyposażony w zintegrowaną klapykę automatycznie otwierającą się podczas wkładania i zamykającą podczas wyjmowania wtyku RJ45 <u>strona PLa</u> – klapyka przeciwkurzowa ma być zintegrowana na płycie czołowej gniazda; jeżeli płyta nie będzie posiadała takowej należy zastosować moduł taki sam jak w panelu krosowym
Czerwony	<b>WLAN z funkcją PoE+</b> <u>strona panelu krosowego</u> - moduł ma być wyposażony w zintegrowaną klapykę automatycznie otwierającą się podczas wkładania i zamykającą podczas wyjmowania wtyku RJ45 <u>strona PLa</u> – klapyka przeciwkurzowa ma być zintegrowana na płycie czołowej gniazda; jeżeli płyta nie będzie posiadała takowej należy zastosować moduł taki sam jak w panelu krosowym
Niebieski	<b>CCTV i KD z funkcją PoE+</b> <u>strona panelu krosowego</u> - moduł ma być wyposażony w zintegrowaną klapykę automatycznie otwierającą się podczas wkładania i zamykającą podczas wyjmowania wtyku RJ45 <u>strona PLa</u> – klapyka przeciwkurzowa ma być zintegrowana na płycie czołowej gniazda; jeżeli płyta nie będzie posiadała takowej należy zastosować moduł taki sam jak w panelu krosowym

Tabela 1. Rodzaje modułów i kabli krosowych RJ45 kat.6A z przeznaczeniem

Dla podłączenia urządzeń peryferyjnych takich jak Access Point WiFi oraz kamera CCTV, lub o podobnym profilu dopuszcza się zakończenie kabla symetrycznego bezpośrednio ekranowanym wtykiem RJ45 kat.6A. Taki sposób realizacji połączenia znacząco upraszcza topologie pod warunkiem spełnienia wymagań opisanych w normie EN 50173-6. Producent oferowanego rozwiązania musi posiadać w swojej ofercie odpowiednie wtyki RJ45 – patrz wymagania szczegółowe dla wtyków RJ45. **Połączenie zrealizowane w topologii MPTL musi zostać poddane pomiarom i certyfikacji w celu uzyskania gwarancji na te łącza.**

Wszystkie nieużywane gniazda RJ45 które pozostają w przestrzeniach ogólnodostępnych oraz wskazane przez Administratora sieci należy zabezpieczyć za pomocą specjalnych blokad wpięcia wtyków RJ45 do portów w kolorze odpowiadającym kolorowi zastosowanego gniazda.



### 5.2.2 Wymagania dla kabli symetrycznych

Ze względu na przyjęte wymiary przepustów kablowych oraz zaprojektowane trakty prowadzenia kabli i związane z tym przeswity, wymagane jest zastosowanie medium transmisyjnego o maksymalnej średnicy zewnętrznej 7,0mm (co determinuje maksymalną średnicę żyły na 23 AWG). Nie dopuszcza się kabli o większej średnicy zewnętrznej. Instalacja ma być poprowadzona podwójnie ekranowanym kablem konstrukcji F/FTP z osłoną zewnętrzną trudnopalną (LSZH).

W związku z potrzebą zapewnienia jak najlepszych parametrów dla szybkich aplikacji 1G/10G i uzyskania najwyższej odporności przed zakłóceniami należy zastosować kable ekranowane kategorii 6<sub>A</sub> o konstrukcji F/FTP (każda para ekranowana za pomocą folii aluminiowej oraz wspólny ekran dla wszystkich par z folii aluminiowej).

#### Minimalne wymagania dla kabla miedzianego F/FTP kategoria 6<sub>A</sub>;

- Średnica zewnętrzna kabla – max. 7.0mm;
- Przekrój żyły przewodnika – 23AWG;
- Minimalny promień gięcia kabla – 4x średnica kabla podczas pracy
- NVP – 72%
- Rodzaj osłony zewnętrznej: LSZH;
- Euroklasa – Dca-s2,d2,a1;
- Gwarancja pełnego wsparcia PoE i zgodności z wymaganiami IEEE 802.3af i IEEE 802.3at, IEEE 802.3bt dla aplikacji PoE i PoE+;
- Temperatura pracy: -20°C do +75°C;
- Zgodność z ISO 11801 Kategoria 6<sub>A</sub>/Klasa E<sub>A</sub>, ANSI/TIA-568-C.2, IEEE 802.3an;
- Certyfikat zgodności normatywnej niezależnego laboratorium dla min. 4 połączeń w kanale do 100m dla ISO 11801 Klasa E<sub>A</sub>;

### 5.2.3 Wymagania dla modułów gniazd RJ45

W opisanie płyty czołowe należy zamontować ekranowane dwuelementowe moduły gniazda RJ45 kat. 6<sub>A</sub>. Moduł gniazda RJ45 ma posiadać konstrukcję dwuelementową, składającą się z części przedniej (z interfejsem RJ45 oraz złączami IDC dla par transmisyjnych) oraz części tylnej. Metalowa obudowa (zarówno na części przedniej i tylnej) podczas montażu gniazda ma się składać w szczelną całość. Konstrukcja modułu nie może zniekształcać konstrukcji kabla, ma również zapewniać maksymalną łatwość instalacji oraz gwarantować najwyższe parametry transmisyjne. Wymaga się, aby każdy moduł gniazda RJ45 posiadał możliwość uniwersalnego terminowania kabli, tj. w sekwencji T568A lub T568B. Każdy moduł ma być zarabiany narzędziami. Wymagane jest, wykorzystanie do montażu takich narzędzi, które terminują gniazdo (wszystkie 8 żył) poprzez jeden ruch narzędzia, zapewniając krótkie rozploty par max. 6mm (a przez to najlepsze możliwe osiągi transmisyjne) oraz dużą powtarzalność i szybkość zarabiania – **tym samym nie dopuszcza się modułów gniazd które terminowane są metodą narzędzia uderzeniowego lub beznarzędziowo.**

Dla zapewnienia w kanale transmisyjnym odpowiednich parametrów dla przesyłu szybkich aplikacji takich jak 1G/10G oraz pełne wsparcie dla najnowszych wymagań PoE należy zastosować moduły ekranowane RJ45 kategorii 6A wysokiej klasy.

#### Minimalne wymagania dla modułów gniazd RJ45:

- Zgodność z ISO 11801 Kategoria 6A/Klasa EA, ANSI/TIA-568-C.2, IEEE 802.3an;
- Wymagany certyfikat na kanał transmisyjny w konfiguracji 4-złączowej do 100m;
- Wymagany certyfikat komponentowy dla modułu RJ45 kat.6A;
- Gwarancja pełnego wsparcia PoE i zgodności z wymaganiami IEEE 802.3af i IEEE 802.3at, IEEE 802.3bt (typ 3 i 4) dla aplikacji PoE, PoE+, PoE++ dla minimum 2500 cykli połączeniowych;
- Wsparcie dla PoH (Power over HDBaseT do 100W);

- Temperatura pracy: -10°C do +65°C;
- Zgodność z ANSI/TIA-1096A; IEC 60603-7, IEC 60512-99-001, RoHS
- Zapewnia ekranowanie 360°C zintegrowane z modułem – bez dodatkowych elementów ekranujących dokładanych do gniazda;
- Zapewnia stabilne połączenie z panelem krosowym w celu prawidłowego uziemienia;
- Producent oferowanych modułów ma mieć dostępne w ofercie:
  - moduły przynajmniej w 6-ciu kolorach do wyboru (3 kolory wykorzystujemy w projekcie + 3 dodatkowe na przyszłe potrzeby);
  - moduły z automatyczną sprężynową zintegrowaną klapką przeciwkurzową zapewniająca ochronę min. IP40 oraz bez klapki (moduły z klapką mają być stosowane w panelach krosowych oraz w gniazdach które nie posiadają w płytach czołowych zintegrowanych zaślepek przeciwkurzowych);
- Każdy moduł ma być przetestowany w 100% przez producenta a następnie indywidualnie oznakowany numerem seryjnym;
- Konstrukcja modułów musi umożliwiać upakowanie do 48 portów w panelu 1U;
- Moduł podczas terminowania ma zapewniać optymalną wydajność poprzez zachowanie geometrii par i zminimalizowanie rozplotu;
- Terminowanie modułu ma zapewniać poprawne umieszczenie przewodników w nożach wykorzystując płynny ruch bez konieczności uderzania w wewnętrzne komponenty modułu;
- Możliwość terminowania 4 par w tym samym momencie;
- Dopuszczalna grubość przewodnika to 22-26AWG, 100Ω w wykonaniu drut i skrętka;
- Moduł musi być oznaczony kolorami w celu łatwego rozpoznania schematu rozszycia T568A i T568B;

Rodzaj testu	Metoda badania	Pomiar	Wynik testów
Siła normalna	-	Obciążenie (gramy)	>100
Trwałość	IEC 512-9a	Rezystancja obwodu (mΩ)	<40
Podłączanie / Odłączanie	IEC 512-3b	Siła podłączenia (N)	<20
		Siła rozłączenia (N)	<20
Cykle terminacyjne	IEC 352	Ilość cykli	>20
Cykle połączeniowe	IEC 60603-7	Liczba możliwych połączeń wtyków	>2500
Wibracje	IEC 512-6d	Rezystancja obwodu (mΩ)	<40
Wstrząsy	IEC 512-6c	Zakłócenia kontaktowe (mikrosekundy)	<5
<b>Testy elektryczne</b>	<b>Pomiar</b>	<b>Rezultat</b>	
Niski poziom rezystancji obwodu	IEC 512-2a	Rezystancja (mΩ)	<20
Napięcie przebicia dielektryka	IEC 512-4a	1000VAC, 1 minuta	Przeszły
Rezystancja izolacji	IEC 512-3a	Rezystancja (MΩ)	>500
Odporność na korozję w wyniku przepływu gazów mieszanych	IEC 512-11g	Rezystancja obwodu (mΩ)	<40
Żywotność w wysokich temperaturach	IEC 512-9b	Rezystancja obwodu (mΩ)	<40
Wilgotność	IEC 512-11c	Rezystancja obwodu (mΩ)	<40
Szok termiczny	IEC 512-11d	Rezystancja obwodu (mΩ)	<40
Sekwencja klimatyczna	IEC 512-11a	Rezystancja obwodu (mΩ)	<40

Tabela 2 Wymagane parametry mechaniczne gniazd RJ45

#### 5.2.4 Wymagania dla wtyków RJ45 (MPTL - zastosowanie opcjonalne)

Dla podłączenia urządzeń peryferyjnych takich jak Access Point WiFi oraz kamera CCTV, lub o podobnym profilu dopuszcza się zakończenie kabla symetrycznego bezpośrednio ekranowanym wtykiem RJ45 kat.6A. Taki sposób realizacji połączenia znacząco upraszcza topologie pod warunkiem spełnienia wymagań opisanych w normie EN 50173-6. Połączenie zrealizowane w topologii MPTL musi zostać poddane pomiarom i certyfikacji w celu uzyskania gwarancji na te łącza.

Dla zapewnienia w kanale transmisyjnym odpowiednich parametrów dla przesyłu szybkich aplikacji takich jak 1G/10G oraz pełne wsparcie dla najnowszych wymagań PoE należy zastosować wtyki ekranowane RJ45 kategorii 6A wysokiej klasy.

### **Minimalne wymagania dla wtyków RJ45:**

- Zgodność z ISO 11801 Kategoria 6A/Klasa EA, ANSI/TIA-568.2-D, IEEE 802.3an;
- gwarancja pełnego wsparcia PoE i zgodności z wymaganiami IEEE 802.3af i IEEE 802.3at, IEEE 802.3bt (typ 3 i 4) dla aplikacji PoE, PoE+, PoE++; HDBASE-T
- Temperatura pracy: -40°C do +85°C;
- Ilość cykli połączeniowych – min. 2500
- Ilość cykli ponownego zaterminowania – min. 20
- Zgodność z IEC 60603-7, RoHS deklaracja zgodności CE
- Klasa szczelności IEC 60529 IP20;
- Fabrycznie wyposażony w zaślepkę przeciwkurzową;
- Wtyk wykonany z cynkowego odlewu ciśnieniowego zapewniający ekranowanie 360° – bez dodatkowych elementów ekranujących dokładanych do wtyku;
- Moduł podczas terminowania ma zapewniać optymalną wydajność poprzez zachowanie geometrii par i zminimalizowanie rozplotu;
- Terminowanie modułu ma zapewniać poprawne umieszczenie przewodników w nożach wykorzystując płynny ruch bez konieczności uderzania w wewnętrzne komponenty modułu;
- Terminowanie wszystkich 4 par w tym samym momencie;
- Wtyk musi mieć prostą konstrukcję która umożliwia zaterminowanie w każdych warunkach;
- Akceptowalna średnica terminowanego kabla: 5.8-9mm
- Dopuszczalna grubość przewodnika dla drutu 22-26AWG (1.0mm-1.6mm);
- Wtyk musi mieć możliwość rozszycia wg. T568A lub T568B;

### **5.2.5 Wymagania dla paneli krosowych okablowania symetrycznego**

Wszystkie kable miedzianego okablowania poziomego należy zakończyć na panelach krosowych prostych o wysokości montażowej 1U i pojemności 48/24.

#### **Minimalne wymagania dla panela krosowego 48 portów:**

- Wysokość montażowa 1U, wersja prosta 19”;
- Fabryczna numeracja u góry każdego portu;
- Maksymalne upakowanie – do 48 portów miedzianych RJ45;
- Panel musi być wyposażony w mechanizmy zatraskowe dla modułów RJ45;
- Montaż i demontaż modułów w panelu musi odbywać się bez specjalistycznych narzędzi;
- Panel krosowy musi umożliwiać także montaż interfejsów multimedialnych na życzenie klienta;
- Wszystkie porty panela krosowego muszą mieć automatyczny kontakt z ekranem modułów RJ45;
- Wszelkie porty panela krosowego, które nie zostaną wykorzystane należy zaślepić zaślepką;
- Panel musi zostać wyposażony z tyłu w półkę z prętami podtrzymującymi kable.

#### **Minimalne wymagania dla panela krosowego 24 porty:**

- Wysokość montażowa 1U, wersja prosta, 19”;
- Fabryczna numeracja każdej sekcji portów u góry panela;
- Miejsca na opisy portów na górze panela;
- Maksymalne upakowanie – do 24 portów miedzianych RJ45;
- Panel musi być wyposażony w mechanizmy zatraskowe dla modułów RJ45;
- Montaż i demontaż modułów w panelu musi odbywać się bez specjalistycznych narzędzi;
- Panel krosowy musi umożliwiać także montaż interfejsów multimedialnych na życzenie klienta;
- Panel krosowy musi posiadać z tyłu zintegrowaną półkę dla mocowania i podtrzymywania kabli wraz z możliwością przypięcia pojedynczych kabli opaskami
- Wszystkie porty panela krosowego muszą mieć automatyczny kontakt z ekranem modułów RJ45;
- Panel musi posiadać wbudowany port dla podłączenia uziemiania;
- Wszelkie porty panela krosowego, które nie zostaną wykorzystane należy zaślepić zaślepką.

**Uwaga:**

**Panele mają być wyposażone w moduły gniazd tego samego typu co w gniazdach dostępowych Użytkownika (PL).**

**5.2.6 Wymagania dla kabli krosowych miedzianych / strona szafy**

Biorąc pod uwagę duże zagęszczenie kabli krosowych należy zastosować kable o zmniejszonym przekroju 28AWG aby usprawnić zarządzanie, poprawić przejrzystość w szafie, zwiększyć dostęp do portów oraz zoptymalizować przepływ powietrza do urządzeń aktywnych (lepsze chłodzenie).

**Minimalne wymagania dla kabli krosowych:**

- Kable krosowe mają być wykonane z linki ekranowanej F/UTP kategorii 6<sub>A</sub> 28AWG;
- Wtyki RJ45 w kablach krosowych muszą być wyposażone w specjalny manager znajdujący się wewnątrz wtyku który nie pozwala aby pary kabla uległy nadmiernemu rozplotowi gwarantując jednocześnie najwyższą wydajność dla kategorii 6<sub>A</sub> i 10GBASE-T;
- Wymagana maksymalna średnica linki to 4,7mm;
- Osłona zewnętrzna kabla krosowego CM/LSZH;
- Zgodność z ANSI/TIA-568.2-D, ANSI/TIA-1096-A, ISO IEC 11801, IEC 60603-7, IEC 60332-1, IEC 60754-2, IEC 61034-2, deklaracja zgodności CE, RoHS, ;
- Piny wtyków wykonane z połączanego fosforobrazu;
- Konstrukcja wtyku musi uniemożliwiać zaczepianie końcówki kabla krosowego podczas wyciągania go z wiązki kabli;
- Kabel krosowy musi zapewniać identyfikowalność (na kablu musi być etykieta z podaną kategorią kabla, jego długością oraz numerem kontroli jakości);
- Kable krosowe muszą wspierać standardy aplikacji PoE IEEE 802.3af/802.3at (48 kabli w wiązce) oraz 802.3bt typ 3 i typ 4 (24 kable w wiązce);
- Minimalna ilość cykli połączeniowych min. 2500;
- Temperatura pracy: -10°C do 75°C
- Wszystkie kable krosowe mają być fabrycznie wykonane i przetestowane na mapę połączeń oraz NEXT i RL;
- Wszystkie komponenty składowe: wtyki, kabel mają być wyprodukowane i trwale oznaczone przez tego samego producenta co cały system okablowania i zostać objęte 25-letnią gwarancją systemową producenta;
- Należy przewidzieć 100% kabli krosowych do podłączeń z obu stron;
- Kable krosowe muszą być dostępne w min. 7 kolorach;
- **Na etapie realizacji należy dostarczyć kable krosowe w kolorach podanych na rysunku nr.1 oraz w tabeli nr. 1 w zależności od przeznaczenia;**
- Dostępna długość kabli krosowych od 0.2m do 40m; Kable krosowe muszą mieć możliwość zastosowania opcjonalnego zabezpieczenia przed wypięciem z gniazda RJ45 min. w 7 kolorach.

**5.2.7 Wymagania dla kabli dołączeniowych / strona użytkownika**

**Minimalne wymagania dla kabli krosowych:**

- Kable krosowe mają być wykonane z linki ekranowanej F/UTP kategorii 6<sub>A</sub> 26AWG;
- Wtyki RJ45 w kablach krosowych muszą być wyposażone w specjalny manager znajdujący się wewnątrz wtyku który nie pozwala aby pary kabla uległy nadmiernemu rozplotowi gwarantując jednocześnie najwyższą wydajność dla kategorii 6<sub>A</sub> i 10GBASE-T;
- Wymagana maksymalna średnica linki to 6,3mm;
- Osłona zewnętrzna kabla krosowego CM/LSZH;
- Zgodność z ANSI/TIA-568.2-D, ANSI/TIS-1096-A, ISO IEC 11801, IEC 60603-7, IEC 60332-1, IEC 60754-1, IEC 61034-2, deklaracja zgodności CE, zgodność z RoHS ;

- Piny wtyków wykonane z połączanego fosforobrazu;
- Konstrukcja wtyku musi umożliwiać zaczeplanie końcówki kabla krosowego podczas wyciągania go z wiązki kabli;
- Kabel krosowy musi zapewniać identyfikowalność (na kablu musi być etykieta z podaną kategorią kabla, jego długością oraz numerem kontroli jakości);
- Kable krosowe muszą wspierać standardy aplikacji PoE IEEE 802.3af/802.3at (min. 48 kabli w wiązce) oraz 802.3bt typ 3 i typ 4 (min. 24 kable w wiązce);
- Minimalna ilość cykli połączeniowych min. 2500;
- Wszystkie kable krosowe mają być fabrycznie wykonane i przetestowane na mapę połączeń oraz NEXT i RL;
- Wszystkie komponenty składowe: wtyki, kabel mają być wyprodukowane i trwale oznaczone przez tego samego producenta co cały system okablowania i zostać objęte 25-letnią gwarancją systemową producenta;
- Należy przewidzieć 100% kabli krosowych do podłączeń z obu stron;
- Kable krosowe muszą być dostępne w min. 7 kolorach;
- **Na etapie realizacji należy dostarczyć kable krosowe w kolorach podanych na rysunku nr.1 oraz w tabeli nr. 1 w zależności od przeznaczenia;**
- Dostępna długość kabli krosowych od 0.2m do 40m;
- Kable krosowe muszą mieć możliwość zastosowania opcjonalnego zabezpieczenia przed wypięciem z gniazda RJ45 min. w 7 kolorach;

### 5.3 Okablowanie szkieletowe

Okablowanie szkieletowe ma zapewnić kanały transmisyjne o dużej przepływności bitowej łączące poszczególne punkty dystrybucyjne sieci ze sobą, oraz dodatkowo zapewnić łączność telefoniczną. Dobór nośników ma zapewnić minimalizację zakłóceń elektromagnetycznych oraz zapewnienia maksymalnej uniwersalności w uruchamianiu różnorodnych protokołów transmisyjnych. Łąca szkieletowe mają tworzyć topologię gwiazdy.

Szkielet pionowy (relacja GPD/PPD) należy zaprojektować z użyciem poniższego zestawu kabli:

- kabla światłowodowego wielomodowego 12-włóknowego kategorii OM3 o konstrukcji luźnej tuby,
- 4 kable miedzianych F/FTP kat.6<sub>A</sub>;

Szkielet telefoniczny (GPD/PPD) należy zaprojektować z użyciem poniższego zestawu kabli:

- Kabel wieloparowy telefoniczny kat.3 – ilość par 100.

We wszystkich panelach krosowych światłowodowych należy zastosować interfejs typu LC.

Od strony szaf GPD/PPD wszystkie numery wewnętrzne należy odzwierciedlić na panelach telefonicznych RJ45 aby umożliwić użytkownikowi szybkie krosowanie z użyciem standardowych kabli krosowych RJ45. Kabel telefoniczny zakańcząć na panelu telefonicznym rozszywając po dwie pary na port.

#### 5.3.1 Wymagania dla kabla światłowodowego wielomodowego

**Minimalne wymagania dla kabla światłowodowego MM OM3 24 włókna:**

- powłoka zewnętrzna kabla – LSZH/LSHF-FR/FRNC zgodna z EN 50290-2-27;
- konstrukcja luźnej tuby z żelem;
- rdzeń ma być zabezpieczony przed wnikaniem wody za pomocą pęczniejącej taśmy;
- włókna w buforze 250µm;
- maksymalna średnica zewnętrzna kabla – 6,5mm;
- minimalny promień gięcia podczas instalacji – 130mm;
- minimalny promień gięcia długoterminowy – 75mm;
- wszystkie włókna w kablu dla łatwej identyfikacji mają mieć inny kolor;

**Parametry mechaniczne**



- Wytrzymałość na rozciąganie (długoterminowe): 340N
- Wytrzymałość na rozciąganie (podczas instalacji): 1200N
- Wytrzymałość na ściskanie: 3000N/100mm
- Wytrzymałość na uderzenie: 100J

**Parametry środowiskowe**

- Temperatura pracy: -20°C do 70°C
- Temperatura instalacji: -20°C do 70°C
- Temperatura przechowywania i transportu: -40°C do 70°C

**Maksymalna tłumienność**

- 3.5dB/km dla fali 850nm
- 1.5dB/km dla fali 1300nm

**Standardy**

- IEC 60332-1-2
- IEC 60332-3-24
- IEC 60754-2
- IEC 61034
- EN50290-2-27
- Euroklasa Dca-s2-d2-a1

### 5.3.2 Wymagania dla obudowy światłowodowej

Obudowa światłowodowa musi mieć konstrukcję pozwalającą na ochronę, organizację, oraz zarządzanie kablami światłowodowymi, spawami, pigtailami, adapterami oraz kablami krosowymi.

**Minimalne wymagania dla obudowy światłowodowej:**

- Musi umożliwiać montaż kaset światłowodowych z adapterami ST, FC, SC, LC, MTRJ, E2000, MPO;
- Musi umożliwiać montaż preterminowanych kaset MPO/LC w różnych konfiguracjach;
- Montaż i demontaż kaset w panelu musi odbywać się beznarzędziowo;
- Obudowa światłowodowa musi umożliwiać także montaż interfejsów RJ45 i multimedialnych na życzenie klienta;
- Obudowa musi mieć wysuwaną szufladę ułatwiającą prace instalacyjne;
- Od tyłu obudowa ma posiadać:
  - po każdej stronie do wyboru po 3 wejścia kabli światłowodowych fabrycznie zaślepionych;
  - po każdej stronie możliwość montażu po 2 elementy odciążające (likwidujące naprężenie kabli przy wejściu do obudowy);
  - dla portów wejścia kabli zaślepki z możliwością dostosowania ich do średnicy wprowadzanego kabla światłowodowego;
- Obudowa 1U/19" musi obsłużyć do 4 kaset i 96 włókien dla adapterów LC;
- Od frontu obudowa musi mieć dodatkowy dystans zabezpieczający przed dostępem do kabli światłowodowych oraz adapterów wraz z uchylną przezroczystą osłoną zamykaną na zamek z możliwością umieszczenia opisów; osłona musi być demontowalna aby nie przeszkadzała podczas instalacji;
- Od tyłu obudowa musi zostać wyposażona w uchylną osłonę zamykaną na zamek posiadającą pola opisowe; osłona musi być demontowalna aby nie przeszkadzała podczas instalacji;
- Od frontu obudowa światłowodowa po obu stronach racka musi mieć zamontowane specjalne klipsy sterujące promieniem gięcia oraz uniemożliwiające uszkodzenie kabli krosowych;
- Obudowa światłowodowa ma być fabrycznie wyposażona w dwie demontowalne szpule organizujące zapas włókien światłowodowych wewnątrz obudowy;
- Obudowa światłowodowa ma być fabrycznie wyposażona w elementy organizujące przebieg kabla wewnątrz obudowy;

- Obudowa 1U ma umożliwiać wewnątrz montaż do 4 tacek na 24 spawy światłowodowe;
- Wszelkie wolne sloty obudowy światłowodowej, które nie zostaną wykorzystane należy zaślepić zaślepką.

### 5.3.3 Wymagania dla kaset światłowodowych

- Kasetka ma być wyposażona w 6 duplexowych adapterów OM3 LC;
- Adaptery mają być zgodne z TIA/EIA-568-C.3, TIA/EIA-604 FOCIS-10;
- Kasetka musi być kompatybilna z obudową światłowodową;
- Montaż oraz demontaż kasety nie może wymagać dodatkowych narzędzi;

#### Dodatkowo w ofercie producenta muszą znaleźć się kasetki

- z adapterami ST, SC, LC, MTRJ, E2000, MPO
- z adapterami dla włókien OM1-OM5, OS1-OS2;
- obsługujące do 24 włókien na 1 kasetkę dla złącz LC;

### 5.3.4 Wymagania dla tac na spawy światłowodowe

- taca ma obsługiwać do 24 spawów;
- możliwość instalacji osłonek spawów 60mm i 45mm;
- taca ma mieć konstrukcję bez ostrych narożników i krawędzi;
- taca ma mieć zintegrowane elementy do układania zapasu włókien światłowodowych dbając o zachowanie odpowiednich promieni gięcia;
- taca musi posiadać uchwyty zabezpieczające przed wypadaniem włókien z tacy;
- taca musi być wyposażona w zamykaną przezroczystą osłonę na zawiasach która chroni włókna i spawy światłowodowe;
- możliwość instalacji tac na spawy piętrowo (jedna na drugą);

### 5.3.5 Wymagania dla pigtaili światłowodowych LC OM3

**Światłowodowe pigtaile LC wielomodowe OM3 muszą spełniać wszystkie poniższe wymagania:**

- osłona zewnętrzna – LSZH;
- kolor osłony: OM3 – aqua
- średnica zewnętrzna – 900um

#### Parametry środowiskowe

- Temperatura pracy: -20°C do 60°C
- Temperatura przechowywania i transportu: -40°C do 70°C

#### Parametry optyczne IL :

- OM3 max. 0,25dB

#### Parametry optyczne RL:

- OM3 min. 26dB

#### Trwałość złączy

- Min. 500 cykli połączeniowych;

#### Normalizacja

- ISO/IEC 11801, TIA/EIA-568-C.3, TIA-604-3 (FOCIS-3), TIA-604-10 (FOCIS-10), IEC 60332-1-2, IEC 60332-3-24, IEC, 60754-1, IEC 60754-2, IEC 61034-2

### 5.3.6 Wymagania dla kabli krosowych światłowodowych OM3

**Światłowodowe kable krosowe LC duplex muszą spełniać wszystkie poniższe wymagania:**

- osłona zewnętrzna – LSZH;
- kolor osłony: aqua

- średnica zewnętrzna – 1,6mm duplex
- minimalny promień gięcia kabla:
  - krótkoterminowo – 16mm
  - długoterminowo – 32mm
- konstrukcja złącza LC duplex wraz z osłoną złącza musi umożliwiać łatwe odłączenie złącza LC od adaptera LC poprzez pociągnięcie za osłonę złącza (boota); takie rozwiązanie jest bardzo przydatne przy dużym zagęszczeniu portów LC z racji na małe gabaryty tego złącza i trudny dostęp; rozwiązanie takie nie może powodować uszkodzenia złącza ani kabla światłowodowego;

**Parametry środowiskowe**

- Temperatura pracy: -10°C do 60°C
- Temperatura przechowywania i transportu: -40°C do 70°C

**Parametry optyczne IL dla złącz:**

- max. 0,10dB

**Parametry optyczne RL dla złącz:**

- min. 26dB

**Trwałość złączy**

- 500 cykli połączeniowych;

**Normalizacja**

- ISO/IEC 11801, TIA-568-C.3, TIA-604-10 (FOCIS-10), zgodność RoHS 2002/95/EC, IEC 60332-1-2, IEC 60332-3-24, IEC 60754-1, IEC 60754-2, IEC 61034-2;

## **5.4 Urządzenia aktywne**

### **5.4.1 Założenia ogólne:**

Struktura sieci lokalnej i jej topologia, odzwierciedla wymaganą strukturę na potrzeby dostarczenia odpowiedniej jakości usług sieciowych, dla systemów Security i innych, między innymi:

- kontroli dostępu,
- systemu CCTV, pracujących z wykorzystaniem protokołów IP, jak i innych elementów systemów bezpieczeństwa obiektu,
- systemów i aplikacji wykorzystywanych, bądź przewidywanych do wykorzystania w przyszłości w budynku, w tym wideokonferencji,
- bezpiecznego dostępu dla użytkowników końcowych,
- systemów telefonii, działających na protokole IP,
- dostępu gościnnego dla użytkowników zdefiniowanych, w ramach polityki bezpieczeństwa, zunifikowanego dla dostępu przewodowego, jak i bezprzewodowego,
- systemów bezpiecznego dostępu do sieci Internet lub/i instytucji zewnętrznych (w celu realizacji systemów backupowych, dostępu do sieci Internet itp.).

Powyższe zapewnione jest nie tylko na podstawie odpowiedniej architektury sieci lokalnej, ale również innych systemów i aplikacji, mających wspierać realizację zunifikowanego, a zarazem bezpiecznego dostępu do sieci komputerowej, na której pracować będą różne systemy i aplikacje, mające rozdzielne funkcjonalności. Zaprojektowana infrastruktura sieciowa musi zapewniać jednolitą platformę sprzętową i programową, w pełni ze sobą zintegrowaną, zapewniającą późniejsze jednolite utrzymanie sieci, jej rekonfigurację i modyfikacje, na potrzeby realizacji potrzeb systemów i aplikacji. Aby zagwarantować pełną kompatybilność całego systemu wszystkie jego komponenty muszą pochodzić od jednego producenta.



Zapewni to jeden punkt zgłaszania ewentualnych usterek bądź problemów konfiguracyjnych oraz spójne warunki świadczenia gwarancji oraz wsparcia serwisowego.

W dalszej części opisu, przedstawione są szczegóły związane z architekturą sieci lokalnej, zarówno przewodowej, jak i bezprzewodowej, wymagania, związane z realizacją poszczególnych warstw sieci lokalnej i zastosowanych urządzeń. Należy zwrócić uwagę, że przedstawione wymagania, są wymaganiami minimalnymi, w celu realizacji bądź umożliwienia w przyszłości podłączenia projektowanych systemów teleinformatycznych, bezpieczeństwa, aplikacji i systemów.

#### **5.4.2 Wymagania szczegółowe dla systemów zarządzania i monitorowania infrastrukturą sieciową i dostępem do sieci LAN i WLAN**

W ramach projektu planuje się wdrożenie systemu zarządzania i monitorowania siecią teleinformatyczną oraz uruchomionymi w sieci usługami. Zasadniczymi zadaniami systemu będą monitorowanie stanu infrastruktury, centralizacja procesów zarządzania i konfiguracji urządzeń sieciowych, kontrolowanie i uwierzytelnianie podłączających się do infrastruktury urządzeń końcowych oraz monitorowanie usług i aplikacji działających w sieci.

System stanowić będzie centralny punkt zarządzania infrastrukturą sieciową poprzez graficzny interfejs WWW. System zarządzania wykorzystywany będzie do konfiguracji urządzeń, wdrażania w nich konfiguracji lokalnych sieci VLAN, śledzenia atrybutów urządzeń zainstalowanych w sieci, takich jak numer seryjny, etykieta zasobu, wersja oprogramowania firmware, typ CPU i pamięć. Wymaga się, aby system umożliwiał podgląd i modyfikacje parametrów wszystkich portów urządzeń sieciowych w zakresie konfiguracji przepustowości, sieci VLAN, metody autentykacji i parametrów protokołu Spanning Tree. System musi w sposób automatyczny wykrywać i lokalizować urządzenia podłączone do sieci, przechowywać ich atrybuty i raportować o ich stanie. System musi prowadzić zautomatyzowaną inwentaryzację urządzeń pracujących w sieci, w szczególności na zarządzanie spisem infrastruktury oraz dokumentacji i aktualizacji danych na temat zmian w infrastrukturze. System wykorzystywany będzie do administracji urządzeniami na poziomie plików konfiguracyjnych, planowania aktualizacji oprogramowania firmware, archiwizacji danych konfiguracyjnych, śledzenia wprowadzanych zmian w konfiguracji oraz przywracania konfiguracji.

System musi pozwalać na automatyczne generowanie reprezentacji wizualnej połączeń sieciowych tworząc mapy topologii sieci.

System posłużyć ma do aktywnego przyznawania dostępu do infrastruktury sieciowej określonym użytkownikom i urządzeniom końcowym w oparciu o informacje pochodzące z serwera usług katalogowych (np. Active Directory) poprzez przyznawanie określonego profilu bezpieczeństwa chroniąc tym samym

infrastrukturę przed nieautoryzowanym dostępem do zasobów sieciowych. System kontroli dostępu musi umożliwiać uwierzytelnienie użytkowników i urządzeń podłączanych do sieci z wykorzystaniem protokołu IEEE 802.1X lub adresu MAC urządzenia.

System służyć będzie do uwierzytelniania:

- komputerów użytkowników,
- użytkowników (w przypadku współdzielonych urządzeń),
- drukarek sieciowych,
- telefonów IP, itp.

System musi zapewniać automatyczne wykrywanie punktów końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i adresów IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, Kerberos) lub żądania RADIUS pochodzących z przełączników dostępowych. Wymaga się, aby dostarczony system umożliwiał wyświetlenie w pojedynczym widoku następujących informacji na temat podłączonego systemu końcowego:

- przypisany adres IP,
- fizyczny adres MAC urządzenia,
- nazwa użytkownika (jeżeli występuje),
- adres IP przełącznika, do którego podłączone jest urządzenie końcowe
- port przełącznika, do którego podłączone jest urządzenie końcowe,
- metoda wykorzystana do uwierzytelniania systemu końcowego,
- stan autoryzacji systemu końcowego,
- czas pierwszego podłączenia się do sieci,
- czas ostatniego podłączenia się do sieci.

Powyższe informacje muszą być dostępne niezależnie czy urządzenie lub użytkownik podłączony jest do infrastruktury sieciowej za pośrednictwem przewodowej sieci LAN czy bezprzewodowej sieci WLAN.

Wymaga się również aby system umożliwiał wymianę informacji z wykorzystaniem interfejsu XML API z innymi systemami sieciowymi.

System musi umożliwiać analizę przepływów sieciowych w warstwach L2 do L7 w sieci wewnętrznej, ze szczególnym naciskiem na identyfikację sesji aplikacji sieciowych. Wdrożenie architektury opartej na przepływach sieciowych powinno umożliwiać w przyszłości monitorowanie i zbieranie danych statystycznych od warstwy L2 do L7 dla każdej pojedynczej zestawianej sesji ruchu sieciowego. Rozwiązanie musi posiadać zestaw sygnatur aplikacji do wykrywania wewnętrznie świadczonych aplikacji (Exchange, SQL, itp.), aplikacji działających w chmurze publicznej (Google, poczta elektroniczna, YouTube, P2P, współdzielenie plików, itp.), a także aplikacji społecznościowych (Facebook, Twitter, itp.) oraz wszelkich

sesji RTP takich jak głos i wideo. Dodatkowo system musi w sposób ciągły monitorować usługi sieciowe uruchomione w sieci Zamawiającego takie jak: DHCP, DNS, NTP, LDAP itp.

Rozwiązanie powinno umożliwiać uzupełnienie, poza niniejszym postępowaniem, infrastruktury o dodatkowe rozwiązanie, dedykowane do zbierania dużej ilości danych typu Netflow, w pełni zintegrowane z niniejszym rozwiązaniem zarządzania.

Warunkiem nadrzędnym jest, aby wszystkie wymienione powyżej funkcjonalności dostępne były za pośrednictwem pojedynczego interfejsu graficznego z poziomu przeglądarki WWW. W ramach zaprojektowanej infrastruktury, nie dopuszcza się dostarczenia rozwiązania spełniającego powyższe wymagania w formie odrębnych rozwiązań zarządzanych z osobna, w pełni nie zintegrowanych ze sobą.

**Poniżej znajdują się szczegółowe wymagania per system zarządzania/monitorowania uwzględniony w ramach niniejszego projektu.**

#### **5.4.3 Wymagania szczegółowe dla systemu zarządzania siecią**

##### Funkcjonalność systemu zarządzania siecią i poszczególnymi urządzeniami

1. Musi zapewniać narzędzie do zarządzania na poziomie systemowym - umożliwiające implementacje dowolnej funkcjonalności wynikającej z karty katalogowej zarządzanego urządzenia.
2. Musi umożliwiać centralne wykonywanie operacji systemowych, takich jak wykrywanie urządzeń, zarządzanie zdarzeniami, rejestrowanie zdarzeń i utrzymanie aplikacji.
3. Musi zapewnić narzędzie umożliwiające szybkie i łatwe określenie fizycznej lokalizacji systemów i użytkowników końcowych oraz miejsca ich podłączenia do sieci.
4. Musi zapewniać możliwości monitorowania całego systemu i wdrażania w nim konfiguracji VLAN.
5. Musi zapewniać kompleksowe wsparcie zdalnego zarządzania dla wszystkich proponowanych urządzeń sieciowych, jak również wszystkich urządzeń zarządzanych przez SNMP MIB-I oraz MIB-II.
6. Do obsługi zdalnej nie może wymagać stosowania żadnych klientów użytkowników końcowych lub oprogramowania typu agent.
7. Musi umożliwiać śledzenie atrybutów urządzeń zainstalowanych w sieci, takich jak numer seryjny, etykieta zasobu, wersja oprogramowania firmware, typ CPU i pamięć.

##### Architektura

1. Musi zapewniać scentralizowane zarządzanie wszystkimi urządzeniami sieci przewodowej.
2. Musi zawierać zintegrowane aplikacje typu plug-in, separujące poszczególne komponenty i uzupełniające możliwości systemu zarządzania.
3. Musi mieć możliwość instalacji, jako maszyna wirtualna.
4. Rozwiązanie musi integrować się ze środowiskiem wirtualnym VMware ESX i ESXi.

### Raportowanie

1. Musi zapewniać możliwości modyfikacji, filtrowania i tworzenia własnych, elastycznych widoków sieci.
2. Musi umożliwiać prezentowanie danych w formie wykresów lub tabelarycznej i pozwalać użytkownikowi na wybór wielu unikatowych identyfikatorów obiektów (OID).
3. Musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń).
4. Musi mieć możliwość generowania szczegółowego wykazu produktów zainstalowanych w sieci, zorganizowany według typu urządzenia.
5. Musi rejestrować dane historyczne o atrybutach urządzenia i raportować jakiekolwiek zmiany w urządzeniu.
6. Musi zapewniać dane historyczne o zmianach w konfiguracji i oprogramowaniu firmware urządzenia.
7. Musi posiadać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania, spisem urządzeń.
8. Musi umożliwiać generowanie szczegółowych raportów dla potrzeb związanych z planowaniem spisu urządzeń sieciowych.
9. Musi zapewniać możliwości analiz na poziomie portu.
10. Musi oferować możliwość tworzenia własnych, dostosowanych do potrzeb raportów przez tworzenie indywidualnych szablonów.

### Narzędzia administracyjne

1. Musi pozwalać użytkownikowi na generowanie w tle zaplanowanych zdarzeń i zadań oraz planowanie terminu ich wykonania.
2. Musi zapewnić narzędzie do podglądu i wyboru obiektów MIB (Management Information Base) z reprezentacji opartej na drzewie, oraz zawierać kompilator dla nowych lub pochodzących od innych dostawców MIB.
3. Musi pozwalać administratorom IT na desygnowanie wybranego personelu do aktywowania/dezaktywowania wcześniej skonfigurowanych polityk w razie potrzeby.
4. Musi umożliwiać prezentowanie szczegółowych informacji konfiguracyjnych, w tym datę i godzinę zapisów konfiguracji, wersję oprogramowania firmware i wielkość pliku konfiguracyjnego.
5. Musi posiadać możliwość pobierania oprogramowania firmware do jednego urządzenia lub do wielu urządzeń jednocześnie.
6. Musi mieć możliwość pobierania obrazów boot PROM do jednego urządzenia lub do wielu urządzeń jednocześnie.
7. Musi posiadać zdolność do przeprowadzania zaplanowanych, rutynowych kopii zapasowych konfiguracji urządzeń.
8. Musi mieć możliwość pobierania szablonów konfiguracyjnych w formacie tekstowym (ASCII) do jednego lub większej liczby urządzeń.
9. Musi zapewniać interfejs sieci Web zawierający narzędzia do raportowania, monitorowania, rozwiązywania problemów i panele zarządzania.

10. Musi zapewniać oparte o sieć Web elastyczne widoki, widoki urządzeń oraz dzienniki zdarzeń dla całej infrastruktury.
11. Musi umożliwiać automatyczną reakcję w czasie rzeczywistym poprzez integrację z rozwiązaniami klasy SIEM oraz IPS.
12. Musi umożliwiać diagnozowanie problemów sieciowych i wydajności poprzez analizy danych NetFlow w czasie rzeczywistym.

#### Bezpieczeństwo

1. Musi obsługiwać uwierzytelnianie RADIUS i LDAP dla użytkowników aplikacji.
2. Musi obsługiwać bezpieczne zarządzanie przełącznikiem przez https.
3. Musi mieć możliwość definiowania polityk:
  - ograniczających poziom pasma,
  - ograniczających liczbę nowych połączeń sieciowych,
  - ustalających pierwszeństwo ruchu w oparciu o mechanizmy QoS warstw 2 i 3,
  - nadających tagi pakietom, poddających kwarantannie poszczególne porty lub sieci VLAN i/lub uruchamiających wcześniej zdefiniowane działania
5. Musi funkcjonować automatycznie gwarantując, że odpowiednie usługi są dostępne dla każdego użytkownika. Niezależnie od miejsca jego logowania do sieci.
6. Musi współpracować z istniejącymi w danej sieci metodami uwierzytelniania, w szczególności z musi obsługiwać uwierzytelnianie oparte o 802.1X, Radius oraz MAC.
7. Musi mieć możliwość natychmiastowego blokowania lub dopuszczania różnych aktywności sieciowych, w tym dostępu do sieci Web, poczty elektronicznej lub wymiany plików p2p.
8. Musi zapewniać dynamiczne, konfigurowalne rozwiązanie powstrzymywania zagrożeń z szeroką gamą opcji reagowania, rejestrowania i audytowania.
9. Musi natychmiastowo identyfikować fizyczną lokalizację i profil użytkownika źródła ataku.
10. Musi mieć możliwość podejmowania działań w oparciu o wcześniej określone polityki bezpieczeństwa, włączając w to zdolność do powiadamiania systemu IDS o podjętych działaniach poprzez komunikat SNMPv3 Trap (Inform).

#### Kontrola

1. Musi zapewniać szczegółową kontrolę na poziomie portów, opartą na typie zagrożenia i zdarzenia.
2. Musi zapewniać szczegółową kontrolę (każdego użytkownika i aplikacji) nad podejrzanymi działaniami i nieuprawnionym zachowaniem sieci.
3. Musi mieć możliwość przypisania „roli kwarantanny” użytkownikowi podłączonemu do portu.
4. Musi umożliwiać izolowanie lub poddawanie kwarantannie atakującego, bez zakłócania pracy innych użytkowników, aplikacji lub systemów krytycznych dla danej organizacji.
5. Musi dynamicznie odmawiać, ograniczać lub zmieniać parametry dostępu użytkownika do sieci. Możliwość przypisywania sieci VLAN, reguł filtrowania warstw L2-L4 oraz QoS na warstwach L2-L4 (DSCP i

802.1p) dla każdej maszyny wirtualnej opartej na przełączniku wirtualnym i wirtualnej grupie portów.

Reguły filtrowania na warstwach L3-L4 i reguły QoS muszą obsługiwać zarówno IPv4, jak i IPv6.

#### Skalowalność

System w początkowej fazie realizacji, objętej niniejszym projektem, musi obsługiwać minimum 5 urządzeń sieciowych i do 50 urządzeń dostępu do sieci bezprzewodowej oraz umożliwiać w przyszłości rozbudowę do min. 25 urządzeń sieciowych – węzłów sieci LAN.

#### **5.4.4 Wymagania szczegółowe dla kompleksowego systemu kontroli dostępu do sieci**

System kontroli dostępu do sieci LAN i WLAN, w pełni zintegrowany, zapewnia realizację zabezpieczeń na poziomie sieciowym, zwiększając poziom bezpieczeństwa i zapobiegania przed zagrożeniami, nieautoryzowanego dostępu do sieci, bądź dostępu do sieci niezgodnie z wymaganą polityką bezpieczeństwa. W tym w ramach systemu realizowany, zgodnie z późniejszą polityką bezpieczeństwa będzie dostęp gościnny, z zapewnieniem dostępu do wybranych zasobów sieciowych i systemów czy do sieci Internet.

#### Funkcjonalność

1. System musi umożliwiać uwierzytelnienie użytkowników i urządzeń podłączanych do sieci lokalnej LAN i sieci bezprzewodowej WLAN z wykorzystaniem:
  - standardu 802.1X
  - adresu MAC urządzenia
  - formularza webowego
2. System musi umożliwiać tworzenie reguł autoryzacji (kontroli dostępu) 802.1X opartych o złożone i wielowarunkowe reguły profili bezpieczeństwa.
3. System powinien aktywnie zapobiegać przed dostępem do sieci nieautoryzowanych użytkowników, zagrożonych punktów końcowych i innych niechronionych systemów.
4. System powinien współpracować z rozwiązaniem Microsoft NAP (Network Access Protection).
5. Musi zapewniać automatyczne wykrywanie punktów końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, Kerberos) lub żądania RADIUS pochodzących z przełączników dostępowych.
6. Musi zapewniać możliwość powiadamiania poprzez Syslog oraz pocztę elektroniczną o sytuacjach krytycznych.
7. System musi umożliwiać wysyłanie powiadomień mailowych z wykorzystaniem protokołu SMTP.
8. System musi posiadać wewnętrzną bazę użytkowników. Baza musi umożliwiać wprowadzanie danych poprzez import danych, wprowadzanie danych przy pomocy interfejsu programistycznego.
9. Rozwiązanie musi wykorzystywać oparte na standardach mechanizmy uwierzytelniania dla potrzeb procesów wykrywania, oceniania, kwarantanny, korygowania i autoryzacji podłączanych systemów końcowych.
10. Rozwiązanie musi obsługiwać uwierzytelnianie RADIUS i/lub LDAP.
11. Rozwiązanie musi obsługiwać lokalną autoryzację MAC.

### Profilowanie urządzeń

1. System musi umożliwiać rozpoznawanie rodzaju urządzeń podłączonych do sieci lokalnej LAN i sieci bezprzewodowej WLAN poprzez analizę informacji pochodzących z co najmniej następujących źródeł: DHCP, HTTP, RADIUS, Network Scan (NMAP), DNS, SNMP.
2. System musi umożliwiać dodawanie rozpoznanych urządzeń do grupy.
3. System na podstawie rodzaju rozpoznanego urządzenia musi umożliwiać różnicowanie poziomu dostępu. Musi istnieć możliwość przyznania określonego dostępu na podstawie informacji o urządzeniu dla co najmniej 500 urządzeń.
4. System musi rozpoznawać co najmniej następujące rodzaje urządzeń:
  - urządzenia z systemem Android,
  - Apple iPad, Apple iPhone, Apple iPod,
  - drukarki,
  - telefony IP,
  - stacja robocza z systemem Microsoft Windows,
  - stacja robocza z systemem MAC OS,
  - stacja robocza z systemem Linux.

### Architektura

1. System musi umożliwiać instalację rozproszoną na wielu serwerach fizycznych i/lub wirtualnych w celu zapewnienia wysokiej niezawodności i możliwości stopniowego zwiększania wydajności systemu – w momencie dostawy na co najmniej dwóch niezależnych serwerach,
2. System musi być dostarczony w formie maszyny wirtualnej (wymagane wsparcie dla VMware ESXi i Hyper-V) obejmującej wszystkie elementy funkcjonalne kontroli dostępu, przy czym zamawiający dopuszcza rozwiązanie, gdzie zarządzanie i monitorowanie systemu zostanie zainstalowane na dedykowanej do tego maszynie wirtualnej.
3. W związku z istotnością systemu dla poprawnego funkcjonowania całej sieci system musi umożliwiać realizację wysokiej dostępności poszczególnych elementów funkcjonalnych typu 1:1 lub N+1.
4. Musi zapewniać rozwiązanie NAC typu out-of-band, które może być zarządzane przez jedną centralną aplikację. Wszystkie urządzenia typu NAC Gateway powinny być zarządzane i monitorowane z jednej, centralnej konsoli.
5. Musi być dostarczone jako maszyna wirtualna lub jako dedykowane rozwiązanie sprzętowe.
6. System musi umożliwiać obsługę co najmniej 500 urządzeń równocześnie podłączonych do sieci lokalnej LAN oraz sieci bezprzewodowej WLAN.
7. Rozwiązanie powinno wspierać możliwość rozbudowy do min. 3000 sesji autoryzacyjnych bez potrzeby rozbudowy systemu o dodatkowe serwery fizyczne lub wirtualne - poprzez dodanie do systemu odpowiednich licencji.
8. System musi umożliwiać rozbudowę w przyszłości o narzędzie do oceny stanu zabezpieczeń systemu końcowego – oczywiście w pełni zintegrowane z systemem i zarządzane poprzez ten sam interfejs WWW.



Ocenianie musi być możliwe zarówno bez dedykowanego agenta instalowanego na stacji końcowej jak i z użyciem agenta. Ocenianie w oparciu o agenta dostępnego powinno być dostępne dla co najmniej komputerów z systemem Windows (2000, XP, Vista, 7, 8, 8.1, Server 2003, Server 2008) i MAC OS X musi umożliwiać następujące testy:

- minimalna wersja agenta,
- test wersji systemu operacyjnego,
- test antywirusa (niezainstalowany/zainstalowany, uruchomiony, zaktualizowany, uruchomione RTP),
- test zapory (uruchomiona/wyłączona) z możliwością automatycznego naprawienia niezgodności,
- test poprawek do systemów Windows (sprawdzanie czy poprawka jest zainstalowana bądź nie),
- test usługi Auto Update z opcją automatycznego naprawienia niezgodności,
- test czasu od ostatniej aktualizacji systemu,
- test wygaszacza ekranu (włączony, zabezpieczony hasłem, z określonym czasem aktywacji,
- test obecności/niewystępowania pliku o określonej nazwie i sumie kontrolnej,
- test wymagający braku występowania albo braku uruchomienia oprogramowania P2P z możliwością automatycznego naprawienia niezgodności,
- test procesu (uruchomiony/nieuruchomiony) z opcją automatycznego naprawienia niezgodności,
- test rejestru dla systemów Windows (obecność klucza/zbioru kluczy o konkretnej nazwie, typie wartości i wartości, równy bądź różny zadanemu),
- test usługi (niezainstalowana/zainstalowana/uruchomiona),
- test aplikacji (sprawdzenie obecności zainstalowanej aplikacji o konkretnej nazwie).

Narzędzie takowe dodatkowo powinno mieć możliwość dowolnego dobierania testów ww. rodzajów tworząc schematy oceniania, które będą aplikowane dla wszystkich grup urządzeń i użytkowników bądź dla wybranej grupy urządzeń i użytkowników. Podczas oceniania systemu końcowego musi być możliwość określenia alternatywnej polityki dostępu do zasobów.

Musi być możliwość określenia oceniania jednorazowego przy wstępnym uwierzytelnianiu bądź oceniania wielokrotnego, o częstotliwości oceniania danej grupy urządzeń i użytkowników w zakresie od minut do tygodni. System końcowy podlegający kwarantannie musi otrzymać informację o testach zakończonych niepowodzeniem wraz ze wskazówkami ich poprawienia.

#### Zarządzanie systemem

1. System musi posiadać graficzny interfejs zarządzania – zarządzanie poprzez przeglądarkę internetową lub dedykowaną aplikację.
2. System musi umożliwiać uwierzytelnienie i autoryzację dostępu do interfejsu zarządzania w oparciu o wewnętrzną bazę użytkowników oraz zewnętrzne repozytorium użytkowników.
3. System musi umożliwiać definiowanie zróżnicowanego poziomu dostępu do interfejsu zarządzania.
4. System musi posiadać panel administracyjny, przedstawiający szczegółowy obraz stanu zabezpieczeń podłączonych lub próbujących się podłączyć systemów końcowych.

#### Zarządzenie dostępem gościnnym



1. System musi umożliwiać realizację dostępu gościnnego do sieci lokalnej LAN i sieci bezprzewodowej WLAN przy pomocy portalu webowego. Formularz musi obsługiwać co najmniej następujące przeglądarki: Microsoft IE, Mozilla Firefox, Safari.
2. Rozwiązanie musi posiadać funkcję portalu rejestracyjnego, aby zapewnić bezpieczne korzystanie z sieci przez gości, bez udziału pracowników działu IT.
3. Możliwość sponsorowania dostępu takie jak sponsorowanie email wraz z portalem dla sponsorów służący do zatwierdzania rejestracji gości.
4. Rejestracja gości powinna umożliwiać powiązanie z bramką SMS celem wysyłania PIN-ów weryfikacyjnych o wybranej długości, mogących składać się z różnego rodzaju znaków.
5. System musi umożliwiać rejestrację przez logowanie do Facebooka. Użytkownik po podaniu danych logowania do serwisu Facebook widzi informacje z publicznego profilu, jakie zostaną pobrane celem rejestracji w sieci.
6. System musi umożliwiać dopasowanie wyglądu portalu wybranym użytkownikom i portalu logowania gościnnego, w tym co najmniej zmianę logo strony logowania i zmianę koloru tła.

#### **5.4.5 Wymagania szczegółowe dla poszczególnych komponentów sieciowych**

Przedstawione zakresy są zakresami minimalnymi do spełnienia, w celu umożliwienia na etapie realizacji funkcjonalności wymaganych w ramach wdrażanych systemów i aplikacji wykorzystywanych na obiekcie. Poniżej znajdują się głównie komponenty sprzętowe, wymagane do zastosowania, przy czym ilości przedstawione są poniżej:

- Przełącznik dostępowy 48 portowy z PoE+ - 3 sztuk;
- Przełącznik dostępowy 48 portowy z PoE+ z portami 10Gb - 4 sztuki;
- Przełącznik dostępowy 24 portowy z PoE+ - 1 sztuka;
- Przełącznik dostępowy 12 portowy - 2 sztuka;
- Punkt dostępowy – 12 sztuk (zarządzanych centralnie przez Kontroler – Zamawiający dopuszcza wariant uruchomienia kontrolera na jednym z punktów dostępowych o ile możliwa będzie obsługa za jego pomocą minimum 30 punktów dostępowych).

Dodatkowo Zamawiający wymaga dostarczenia wkładek optycznych w ilościach i typach wyszczególnionych poniżej.

- moduł światłowodowy SR SFP+ - 12 sztuk;
- moduł światłowodowy do stosów SR SFP+ - 16 sztuk lub kable DAC o długości minimum 1m.

Każdy z przełączników powinien dodatkowo mieć kable zasilające oraz być objęty wieczystą gwarancją producenta:

- a. bezpłatne aktualizacje Firmware (minor i major Release)

- b. wymianę uszkodzonego komponentu z wysyłką następnego dnia roboczego od uznania awarii
- c. wsparcia technicznego producenta od poniedziałku do piątku w godzinach 8-17
- d. dostęp do bazy wiedzy producenta

#### Przełącznik dostępowy

#### Wymagania ogólne dla urządzeń typu Przełącznik dostępowy

1. Wysokość urządzenia 1U
2. Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az na wszystkich portach 10/100/1000BASE-T
3. Wbudowany dodatkowy interfejs do zarządzania poza pasmem - out of band management.
4. Przełącznik musi posiadać wbudowany zasilacz 230V AC, oraz musi posiadać możliwość realizacji redundancji zasilania poprzez instalację wewnętrznego lub zewnętrznego dodatkowego zasilacza.
5. Możliwość łączenia do 8 przełączników w stos. Dodatkowo musi posiadać możliwość realizacji stosów z wykorzystaniem wbudowanych portów 10G na duże odległości za pomocą standardowych wkładek 10GBase-SR/LR oraz włókien światłowodowych
6. Tablica MAC adresów min. 16k
7. Pamięć operacyjna: min. 1GB pamięci DRAM
8. Pamięć flash: min. 4GB pamięci Flash oraz bufora pakietów min. 1,5MB
9. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
10. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
11. Obsługa Quality of Service (IEEE 802.1p, DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym)
12. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
13. Możliwość monitorowania zajętości CPU

#### Obsługa Routingu IPv4

14. Pojemność tabeli routingu min. 480 wpisów
15. Routing statyczny
16. Obsługa routingu dynamicznego IPv4
  - a. RIPv1/v2

- b. Możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania

#### 17. Policy Based Routing dla IPv4

##### Obsługa Routingu IPv6

18. Pojemność tabeli routingu min. 240 wpisów

19. Routing statyczny

20. Obsługa routingu dynamicznego dla IPv6

- a. RIPng
- b. Możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla OSPFv3 (np. poprzez dodatkową licencję)

21. Policy Based Routing dla IPv6

##### Obsługa Multicastów

22. Obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration)

23. Obsługa IGMP v1/v2/v3 oraz IGMP v1/v2/v3 snooping

##### Bezpieczeństwo

24. Obsługa Network Login

- a. IEEE 802.1x
- b. Web-based Network Login
- c. MAC based Network Login

25. Obsługa wielu klientów (min. 8) Network Login na jednym porcie (Multiple supplicants)

26. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z systemu NAC

27. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login

28. Musi działać w architekturze bezpieczeństwa opartej o role. Zapewniając ciągłe zarządzanie tożsamościami z uwierzytelnianiem opartym o role, autoryzacją, QoS i ograniczaniem poziomu pasma

29. Urządzenie musi wspierać profile bezpieczeństwa definiowane per użytkownik. Profil bezpieczeństwa oznacza połączenie:

- a. definicji sieci VLAN,
- b. reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,
- c. realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,
- d. realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.

30. Obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) – również per-command Authentication

31. Bezpieczeństwo MAC adresów

- a. ograniczenie liczby MAC adresów na porcie

- b. zatrzaśnięcie MAC adresu na porcie
- c. możliwość wpisania statycznych MAC adresów na port/vlan
- d. możliwość wyłączenia MAC learning

32. Zabezpieczenie przełącznika przed atakami DoS

- a. Networks Ingress Filtering RFC 2267
- b. SYN Attack Protection
- c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania

33. Dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika)

34. Obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation

35. Obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard

Bezpieczeństwo sieciowe

36. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania

37. Obsługa STP, RSTP, MSTP, PVST+

38. Obsługa EAPS (RFC 3619) oraz G.8032

39. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów

40. Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników.

Zarządzanie

41. Zarządzanie przez SNMP v1/v2/v3

42. Obsługa SYSLOG z możliwością definiowania wielu serwerów

43. Sprzętowa obsługa sFlow

44. Obsługa RMON (RFC 1757) i RMON2 (RFC 2021)

Inne

45. Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych)

46. Możliwość uruchamiania skryptów

- a. Ręcznie
- b. O określonym czasie lub co wskazany okres czasu
- c. Na podstawie wpisów w logu systemowym

**5.4.6 Wymagania szczegółowe dla urządzeń typu Przełącznik dostępowy 48 portowy POE+**

Wszystkie zapisy ogólne dotyczące urządzeń typu Przełącznik dostępowy i dodatkowo:

1. Przełącznik posiadający minimum 48 portów 1G 100/1000BASE-T POE+

2. Przełącznik posiadający minimum 8 porty 1G SFP (4 z nich mogą być typu Combo z portami RJ45 POE+)
3. Przełącznik mający możliwość rozbudowy (licencje – np. kosztem portów SFP lub za pomocą dodatkowego modułu) o 4 porty 10G SFP+, lub być dostarczonym od razu w konfiguracji minimum 48 portów 1G 100/1000BASE-T POE+ i minimum 4 porty 10G SFP+.
4. Nieblokującą architekturę o wydajności przełączania min. 176 Gb/s
5. Szybkość przełączania min. 130 Milionów pakietów na sekundę
6. W chwili dostawy musi gwarantować dostarczenie 740W mocy POE oraz standaryzację negocjacji zasilania za pomocą LLDP/LLDP-MED.
7. Dodatkowo musi mieć możliwość, poprzez instalację dodatkowego zasilacza dostarczenie 30W mocy równocześnie na wszystkich 48 portach (1440W POE per przełącznik).

#### **5.4.7 Wymagania szczegółowe dla urządzeń typu Przełącznik dostępowy 48 portowy POE+ z portami 10Gb**

Wszystkie zapisy ogólne dotyczące urządzeń typu Przełącznik dostępowy i dodatkowo:

1. Przełącznik posiadający minimum 48 portów 1G 100/1000BASE-T POE+
2. Przełącznik posiadający minimum 6 portów 1G SFP (4 z nich mogą być typu Combo z portami RJ45 POE+)
3. Przełącznik posiadający 2 porty 10G SFP+
4. Przełącznik mający możliwość rozbudowy (licencje – np. kosztem portów SFP lub za pomocą dodatkowego modułu) o 2 porty 10G SFP+, lub być dostarczonym od razu w konfiguracji minimum 48 portów 1G 100/1000BASE-T POE+ i minimum 4 porty 10G SFP+.
5. Nieblokującą architekturę o wydajności przełączania min. 176 Gb/s
6. Szybkość przełączania min. 130 Milionów pakietów na sekundę
7. W chwili dostawy musi gwarantować dostarczenie 740W mocy POE oraz standaryzację negocjacji zasilania za pomocą LLDP/LLDP-MED.
8. Dodatkowo musi mieć możliwość, poprzez instalację dodatkowego zasilacza dostarczenie 30W mocy równocześnie na wszystkich 48 portach (1440W POE per przełącznik).

#### **5.4.8 Wymagania szczegółowe dla urządzeń typu Przełącznik dostępowy 24 portowy z PoE+**

Wszystkie zapisy ogólne dotyczące urządzeń typu Przełącznik dostępowy i dodatkowo:

1. Przełącznik posiadający minimum 24 porty 1G 100/1000BASE-T POE+
2. Przełącznik posiadający minimum 8 porty 1G SFP (4 z nich mogą być typu Combo z portami RJ45 POE+)

3. Przełącznik mający możliwość rozbudowy (licencje – np. kosztem portów SFP lub za pomocą dodatkowego modułu) o 4 porty 10G SFP+, lub być dostarczonym od razu w konfiguracji minimum 24 porty 1G 100/1000BASE-T POE+ i minimum 4 porty 10G SFP+.
4. Nieblokującą architekturę o wydajności przełączania min. 128 Gb/s
5. Szybkość przełączania min. 95 Milionów pakietów na sekundę
6. W chwili dostawy musi gwarantować dostarczenie 380W mocy POE oraz standaryzację negocjacji zasilania za pomocą LLDP/LLDP-MED.

#### **5.4.9 Wymagania szczegółowe dla urządzeń typu Przełącznik 12 portowy**

Wszystkie zapisy ogólne dotyczące urządzeń typu Przełącznik dostępowy i dodatkowo:

1. Przełącznik posiadający 12 portów 1G 100/1000BASE-T
2. Przełącznik posiadający 2 porty 1G SFP
3. Przełącznik posiadający 2 porty 10G SFP+
4. Przełącznik mający możliwość rozbudowy (licencje – np. kosztem portów SFP, lub za pomocą dodatkowego modułu) o 2 porty 10G SFP+, lub być dostarczonym od razu w konfiguracji 12 portów 100/1000BASE-T i 4 porty SFP+
5. Nieblokującą architekturę o wydajności przełączania min. 104 Gb/s
6. Szybkość przełączania min. 77 Milionów pakietów na sekundę

#### **5.4.10 Wymagania szczegółowe dla urządzeń Punkt dostępowy**

1. Musi mieć możliwość pracy niezależnej (Standalone) oraz pracy z kontrolerem WLAN;
2. Musi obsługiwać standard 802.11ac;
3. Musi posiadać dwa niezależne moduły radiowe pracujące w częstotliwościach 2,4 GHz i 5 GHz;
4. Musi obsługiwać 2x2:2 MIMO;
5. Musi obsługiwać modulację 256 QAM;
6. Musi obsługiwać 8 SSID per moduł radiowy (16 per AP);
7. Musi obsługiwać minimum 250 Klientów per AP;
8. Musi posiadać anteny – minimum 4dBi dla 2,4GHz, 6dBi dla 5GHz;
9. Musi posiadać minimum 1 port Gigabit Ethernet;
10. Musi posiadać funkcjonalność równomiernego dystrybuowania Klientów pomiędzy punktami dostępowymi i pasmami częstotliwościowymi;
11. Musi wspierać standard 802.11r Fast Roaming;
12. Musi wspierać mechanizm wykrywający zakłócenia i automatycznie dostosowywać do nich kanał pracy

oraz moc sygnału;

13. Musi umożliwiać konfigurowanie routingu L3, NAT-a oraz PAT-a;
14. Musi być wyposażony w firewall typu stateful; filtrowanie IP;
15. Musi umożliwiać konfigurację 802.1x, 802.11i, WPA, WPA2;
16. Musi mieć możliwość dostępu poprzez usługi Dynamic DNS;
17. Musi mieć możliwość uruchomienia serwera DHCP;
18. Musi realizować usługi RADIUS;
19. Musi realizować funkcjonalności związane z bramą VPN;
20. Musi posiadać wbudowanego klienta tunelu L2TPv3, oraz IPsec;
21. Musi wspierać OSPF, VRRP, oraz PBR (Policy Based Routing);
22. Musi realizować QoS – minimum WMM, 802.1p, Diffserv i TOS;
23. Musi realizować funkcjonalność Storm Control;
24. Musi wspierać protokoły CDP oraz LLDP;
25. Wbudowana widoczność i kontrola aplikacji w oparciu o DPI (Deep Packet Inspection):
  - minimum 200 reguł;
  - możliwości tworzenia własnych sygnatur aplikacji;
26. Obsługa funkcjonalności rozpoznawania podłączonych urządzeń (Device Fingerprinting);
27. Musi umożliwiać integrację z Ekahau i Aeroscout;
28. Musi umożliwiać wykorzystanie usług lokalizacyjnych do określenia położenia ludzi i zasobów, a także kontroli dostępu do sieci i aplikacji;
29. Musi posiadać wsparcie dla protokołu Bonjour;
30. Musi mieć możliwość uruchomienia usługi Captive Portal;
31. Musi umożliwiać uruchomienie usługi hotspot;
32. Musi posiadać wbudowany IDS;
33. Musi posiadać sensor WIPS możliwy do uruchomienia na obu radiach;
34. Musi posiadać certyfikat kompatybilności Wi-Fi Alliance;
35. Musi wspierać technologię MIMO Power Save;
36. Musi posiadać możliwość zasilania 48V;
37. Temperatura pracy od 0° C do 40° C.

## **5.5 Punkty dystrybucji okablowania strukturalnego**

### **5.5.1 Szafy dystrybucyjne**

W szafach dystrybucyjnej będzie instalowany osprzęt połączeniowy oraz sprzęt aktywny. Szafy oraz wszelkie akcesoria do nich (organizery, zaślepki, listwy zasilające PDU ) muszą pochodzić z oferty tego samego producenta co okablowanie strukturalne.

#### **5.5.1.1 Wymagania dla szaf GPD i PPD**

— Zgodność ze standardem: EIA-310-E / TIA/EIA-942



- Wysokość 42U,
- Szerokość 800mm,
- Głębokość 1000mm dla PPD – 1 sztuka,
- Głębokość 1200mm dla GPD – 2 sztuki,
- Obudowa szafy wykonana z zespawanej i zmontowanej konstrukcji stalowej,
- Wytrzymałość statyczna min. 1360kg na nóżkach i 500kg na kółkach (opcja),
- Wszystkie 4 profile / słupy montażowe o rozstawie 19” muszą umożliwiać regulację w przód i w tył tak aby umożliwić montaż sprzętu zarówno sieciowego jak i serwerowego; wewnątrz szafy musi znajdować się podziałka umożliwiająca precyzyjne ustawienie szyn w pionie,
- Słupy montażowe muszą posiadać oznaczenia każdego U w szafie aby ułatwić planowanie i montaż urządzeń,
- Konstrukcja szafy o szerokości 800mm musi umożliwiać pionowy montaż w przestrzeni bocznej między rakiem a ścianą szafy paneli krosowych 19”- minimalne wymagane upakowanie paneli 19” – 4 sztuki ,
- Drzwi przednie wypukłe jednoskrzydłowe z perforacją min.69% z możliwością montażu prawo i lewostronnego, z dwustopniowym zamkiem i klamką,
- Drzwi tylne dwuskrzydłowe z perforacją min.69% z trójstopniowym zamkiem i klamką,
- Szafy muszą być wyposażone w panele boczne dzielone poziomo aby zapewniać swobodny dostęp do urządzeń,
- Wszystkie elementy rozłączne tj. drzwi, ściany boczne itd. mają posiadać linki uziemiające,
- W dachu muszą znajdować się min. 4 otwory z zaślepkami z włókniną umożliwiające wprowadzenie kabli:
- Szafa ma posiadać uchwyt do montażu minimum dwóch pionowych listw PDU o pełnej wysokości,
- Szafa musi umożliwiać montaż dwóch listw PDU o pełnej wysokości na jednej stronie szafy,
- Każda szafa musi zostać wyposażona min. w jedną listwę zasilającą po min. 9 gniazd;
- Szafa ma posiadać nóżki regulowane, z możliwością wypoziomowania szafy,
- Wszelkie niewykorzystane przestrzenie w szafie należy zaślepić poziomymi zaślepkami,
- Po bokach szaf IDF należy zastosować pionowe organizery 40U z pokrywą;
- Organizery poziome z pokrywkami należy zastosować zgodnie ze sztuką w zależności od przyjętej metody montażu urządzeń w szafie.

### 5.5.2 Listwy zasilające PDU

Inteligentne listwy zasilające PDU to znacznie więcej niż tylko listwa dystrybuująca zasilanie i licznik energii. Listwy PDU monitorują zasilanie w serwerowni i warunki środowiskowe na poziomie szafy, poprzez ciągłe skanowanie potencjalnych przeciążeń obwodów elektrycznych i parametrów dotyczących otoczenia które mogłyby spowodować uszkodzenie kosztownego sprzętu IT. PDU dostarczają wszechstronnych, dokładnych pomiarów energii użytej do zasilania sprzętu IT w celu efektywnego wykorzystania zasobów. Daje to możliwość planowania efektywnego wykorzystania zasobów zasilania, polepsza czas reakcji i umożliwia budowanie serwerowni efektywnie zużywających energię, oszczędnych i przyjaznych środowisku. Podjęcie właściwego wyboru co do sprzętu IT jest podstawą bezpiecznego i efektywnego działania serwerowni. Dobry wybór PDU, sensorów środowiskowych i podwójnie zabezpieczonych kabli zasilających jest kluczem do spełnienia najwyższych wymagań stawianych serwerowniom.

**Listwy dla dystrybucji zasilania w szafach PDU muszą spełniać poniższe wytyczne:**

- Producent musi oferować listwy PDU zarówno w wersji montażu pionowej jak i poziomej 19”;
- PDU muszą wytrzymać temperaturę do 60°C przy pełnym obciążeniu na wszystkich gniazdach;
- PDU o dużej gęstości upakowania gniazd (do 48 sztuk) na jednym profilu o wymiarach max. 1821.2mm x 50.8mm x 111.8mm (musi zmieścić się do szafy 42U) dla zminimalizowania przestrzeni i zmaksymalizowania przepływu powietrza w szafie;
- Szerokość listw pionowych max. 50,8mm;
- Możliwość wymiany kontrolera z wyświetlaczem w trakcie pracy listwy PDU (Hot-Swap);
- Kontroler PDU z wyświetlaczem musi mieć możliwość obrotu o 180° w zależności od strony na której jest montowana listwa;
- Kontroler musi posiadać jasny wyświetlacz OLED z wysokim współczynnikiem kontrastu;



- Redundantny dostęp sieciowy 1Gb/s w konfiguracji 2N dla redundancji połączeń w sieci lub połączeniu do sieci różnych użytkowników;
- Przełączanie gniazd zasilających i krytycznych funkcji PDU musi odbywać się za pośrednictwem HTTPS/TLS, a nie SSL;
- Musi być obsługiwane bezpieczne monitorowanie sieci, aby uniknąć wtargnięć - cała komunikacja danych powinna obsługiwać bezpieczne funkcje RESTful API przez HTTPS/TLS z wykorzystaniem otwartego, niezastrzeżonego standardu branżowego;
- Musi obsługiwać standard Redfish API;
- Gniazda zasilające muszą obsługiwać najnowsze zabezpieczenia i spełniać rygorystyczne wymagania bezpieczeństwa narzędzi do skanowania:
  - HPE WebInspect Security;
  - Tenable Nessus;
  - DDI Frontline;
  - BackTrack Linux Security Editor;
- PDU musi obsługiwać kodowane oznaczone kolorami gniazda PDU w celu identyfikacji każdej z faz z kolorowymi bezpiecznikami automatycznymi;
- PDU musi obsługiwać połączenie sieciowe 1Gb/s i umożliwiać połączenie do 4 listw PDU w celu oszczędzania adresów IP;
- Montaż listw PDU musi odbywać się bez użycia narzędzi i umożliwiać regulowanie położenia jednostki PDU;
- Graficzny interfejs użytkownika jednostki PDU musi dostosowywać się do rozdzielczości ekranu urządzenia użytkownika w celu uzyskania optymalnego interfejsu na urządzeniach mobilnych i tabletach;
- Kodowane gniazda IEC są kompatybilne z bezpiecznymi kablami zasilającymi z blokowaniem W i V z dodatkowym zabezpieczeniem za pomocą standardowych opasek kablowych;
- Minimum 3-letnia standardowa gwarancja producenta z możliwością rozszerzenia do 5-lat;
- Skalowalność pod względem zarządzania urządzeniem za pomocą lokalnego serwera WWW do systemu DCIM w celu monitorowania energii i mocy u jednego dostawcy;
- Obsługa portu USB umożliwiającego szybkie instalowanie oprogramowania wbudowanego i poprawek zabezpieczeń bez wyłączania niezgodnych urządzeń w sieci;
- Musi istnieć możliwość wyłączenia portu USB do udostępniania za pomocą blokady programowej w celu ochrony przed włamaniami;
- Monitorowanie zużycia energii z dokładnością do +/-1% zapewniające dokładność rozliczeniową zgodnie ze specyfikacjami IEC;
- Pomiary muszą obejmować odczyty V, A, VA, W, kWh i PF;
- Obsługa wysokiej niezawodności hydrauliczno-magnetycznych wyłączników awaryjnych stabilnych w temperaturze 60°C;
- Monitorowane Wejścia (MW) - jednostka PDU z możliwością monitorowania potencjalnej agregacji mocy po to aby szybko zidentyfikować potencjalne problemy z zasilaniem i odzyskać dostępną lub niewykorzystaną moc;
- Spełnia globalne standardy zgodności zasilania: UL, cULus, CE i EAC;
- Obsługa monitorowania rozgałęzionych obwodów i równoważenia obciążenia każdego obwodu;
- Obsługa gniazd naprzemiennych;
- Wyświetlanie wszystkich faz jednocześnie na wyświetlaczu OLED podczas ręcznego gromadzenia danych;
- PDU musi natywnie obsługiwać różne czujniki i rozwiązania kontroli dostępu za pośrednictwem tej samej jednostki PDU bez zewnętrznego urządzenia bramowego;
- Razem z PDU należy dostarczać cyfrowe czujniki środowiskowe.:
  - 3x temperatura + wilgotność;
  - Punktowy czujnik zasilania;
- W ofercie producenta listw PDU muszą być dostępne dodatkowe czujniki do wykorzystania w przyszłości:
  - Temperatury;
  - Temperatury + wilgotności;
  - Liniowy czujnik zasilania;
  - Wejście styku bezpotencjałowego;

- Kontaktron drzwiowy;
- HUB dostępowy dla kontroli dostępu do szafy (wymagana obsługa technologii kart 125kHz i 13,56MHz);
- Listwa oświetleniowa LED;
- HUB rozszerzenia portów sensorów

— Obsługa interfejsu bezprzewodowego za pomocą klucza sprzętowego sieci bezprzewodowej;

### 5.5.3 Organizery poziome

Wszystkie projektowane szafy GPD i PPD zostaną wyposażone w organizery poziome z pokrywą na zawiasach zabezpieczającą przed wypadaniem kabli krosowych. Organizery poziome mają mieć wysokość 1U lub 2U i przynajmniej po 12 wejść z góry i z dołu na kable krosowe. W tylnej części organizera mają znajdować się przynajmniej 2 wyloty owalne na wyprowadzenie kabli krosowych do tyłu; krawędzie wylotów muszą być zabezpieczone w taki sposób aby kable krosowe nie były narażone na ostre krawędzie. Skrajne boczne prowadnice kablowe muszą mieć kształt zapewniający odpowiedni promień gięcie kabli krosowych oraz nie narażać ich na ostre krawędzie.

### 5.5.4 Organizery pionowe

Szafy GPF i PPD zostaną wyposażone w pionowe organizery kablowe 40U zamontowane po obu stronach szafy. Organizery zapewniają prawidłowe zarządzanie kablami krosowymi miedzianymi i światłowodowymi podczas krosowania w pionie oraz w połączeniu z organizerami poziomymi stanowią dopełnienie systemu. Pojemność organizera została dobrana w taki sposób aby obsłużyć projektowaną ilość i rodzaj kabli krosowych (40Ux83x76) wraz z min.50% zapasem przestrzeni na przyszłość. Konstrukcja organizera musi zapewniać na pełnej wysokości wejścia na kable krosowe przynajmniej co 25mm oraz posiadać zakładaną pokrywę od frontu która zabezpiecza wypadaniu kabli z organizera.

## 6 Administracja

Wszystkie kable powinny być oznaczone numerycznie, w sposób trwały, zarówno od strony gniazda PL, jak i od strony szafy montażowej. Te same oznaczenia należy umieścić w sposób trwały na gniazdach telekomunikacyjnych w obszarach roboczych oraz na panelach krosowych.

Konwencja oznaczeń okablowania poziomego:

**X / Y . C**

gdzie:

X – identyfikator szafy, G.1.1 – szafa MDF1.1

Y – numer panela krosowego w szafie,

C – numer portu w panelu.

## 7 Gwarancja oraz wymagania dotyczące kompetencji

**Gwarancja na system okablowania strukturalnego ma spełniać poniższe warunki:**

- gwarancja ma być jednolitą bezpłatną usługą serwisową świadczoną przez producenta okablowania (tj. bez ponoszenia jakichkolwiek kosztów przez Użytkownika w przyszłości związanych z przeglądami, serwisowaniem czy innymi pracami związanymi z naprawą i powtórą instalacją wadliwych elementów);
- ma obejmować całość okablowania miedzianego oraz światłowodowego wraz z kablami krosowymi i innymi elementami niezbędnymi do budowy sieci takimi jak panele krosowe, gniazda RJ45, adaptery światłowodowe, pigtaile itp.;
- minimalny czas trwania gwarancji systemowej to 25 lat,
- gwarancja ma być udzielana na oficjalnych warunkach, ogólnie znanych i opublikowanych;
- gwarancja ma być udzielona przez producenta okablowania bezpośrednio Inwestorowi / Użytkownikowi.

### 7.1 Obowiązki producenta okablowania

Producent systemu okablowania w swojej gwarancji systemowej ma zapewniać:

- gwarancję materiałową (w przypadku wykrycia wady lub usterki fabrycznej, produkty wadliwe zostaną naprawione bądź wymienione);
- gwarancję parametrów łącza/kanalu (parametry łącza stałych bądź kanałów będą przewyższać wskazaną klasę okablowania w ciągu trwania całego okresu gwarancyjnego);
- gwarancję aplikacji (protokoły sieciowe współczesne i stworzone w przyszłości, które zaprojektowane były lub będą dla systemów okablowania danej klasy będą działać poprawnie w ciągu całego okresu gwarancyjnego).

**Uwaga:**

**Na życzenie Inwestora/Użytkownika instalacja ma być nadzorowana w trakcie budowy przez inżynierów ze strony producenta.**

Zbudowana infrastruktura kablowa ma być ostatecznie fizycznie sprawdzona przez producenta przed wystawieniem certyfikatu gwarancyjnego pod kątem technicznym, funkcjonalnym oraz estetycznym. Użytkownik/Inwestor musi otrzymać raport, potwierdzający sprawdzenie instalacji oraz ma prawo uczestniczyć w procesie jej weryfikacji.

## **7.2 Obowiązki instalatora**

W celu ujawnienia procedury, jak również zapoznania Użytkownika/Inwestora z prawami, obowiązkami i ograniczeniami gwarancji, wykonawca ma posiadać aktualną umowę zawartą bezpośrednio z producentem okablowania regulującą uprawnienia, procedury, warunki i tryb udzielenia gwarancji Użytkownikowi.

W celu weryfikacji aktualnego statusu certyfikowanego instalatora Producent oferowanego systemu musi udostępniać informację o aktualnym stanie aktywnych certyfikowanych instalatorów na swojej stronie internetowej lub pisemnie na życzenie Inwestora.

Wykonawca ma posiadać na dzień składania oferty status aktywnego certyfikowanego instalatora oraz zatrudniać przynajmniej 2-óch pracowników przeszkolonych w zakresie:

- instalacji, pomiarów, nadzoru, wykrywania oraz eliminacji uszkodzeń wg. programy szkoleń Producenta;

Powyższe kursy mają znajdować się w oficjalnej ofercie producenta.

Dokumenty mają być przedstawione Zamawiającemu przed podpisaniem umowy.

Dostarczone elementy pasywne składające się na system okablowania strukturalnego muszą być oznaczone nazwą lub znakiem firmowym tego samego producenta okablowania i pochodzić z jednolitej oferty rynkowej, będącej kompletnym systemem w takim zakresie, aby zostały spełnione warunki niezbędne do uzyskania gwarancji w/w producenta.

## **8 Odbiór i pomiary sieci okablowania strukturalnego**

Warunkiem koniecznym dla odbioru końcowego instalacji przez Inwestora jest spełnienie wszystkich poniższych warunków:

- wykonanie instalacji w sposób estetyczny, zgodny ze sztuką i obowiązującymi normami,
- wykonanie kompletu pomiarów,
- opracowanie i przekazanie dokumentacji powykonawczej Inwestorowi,
- uzyskanie gwarancji systemowej producenta okablowania.

Wykonawstwo pomiarów sieci miedzianej klasy E<sub>A</sub> powinno być zgodne z normą IEC 61935-1. Pomiary sieci światłowodowej powinny być wykonane zgodnie z normą ISO/IEC 14763-3. Pomiary łącz szkieletowych telefonicznych przetestować na zasadzie działania aplikacji telefonicznych np. Voice 1p/2p. Pomiary należy wykonać dla wszystkich interfejsów okablowania poziomego oraz szkieletowego.

Należy użyć miernika dynamicznego (analyzera), który posiada możliwość analizy parametrów, według aktualnie obowiązujących norm. Sprzęt pomiarowy musi posiadać aktualną kalibrację/legalizację (tj. certyfikat potwierdzający dokładność jego wskazań, wydany przez serwis producenta).

Na raportach pomiarowych muszą się znaleźć informacje dotyczące ustawień sprzętu pomiarowego (norma, typ kabla itp.), nazwa mierzonego łącza oraz wyniki pomiarów wraz z zapasami w stosunku do limitów z norm. Każdy wynik musi być jednoznacznie opisany jako poprawny lub niepoprawny.

### 8.1 Pomiary okablowania miedzianego

- Analizator okablowania wykorzystany do pomiarów sieci miedzianej musi charakteryzować się przynajmniej V klasą dokładności dla klasy E<sub>A</sub> wg IEC 61935-1 (proponowane urządzenia to np. FLUKE DSX5000 lub DSX8000).
- Pomiary sieci miedzianej dla Klasy E<sub>A</sub> należy wykonać na zgodność z ISO/IEC11801 lub EN50173-1 zachowując następującą kolejność:
  1. Łącze stałe (Permanent Link) przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego,
  2. Kable krosowe przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego,
  3. Kanał (Channel) przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego,
- Pomiary łączy wykorzystujących wtyki MPTL należy wykonać zgodnie ANSI-TIA568.2-D wykorzystując odpowiednie adaptery pomiarowe specyfikowane przez producenta sprzętu pomiarowego dla danej klasy okablowania,
- Protokół pomiarowy każdego toru transmisyjnego poziomego miedzianego ma zawierać:
  - mapę połączeń,
  - długość połączeń i rezystancje par,
  - opóźnienie propagacji oraz różnicę opóźnień propagacji,
  - tłumienie,
  - NEXT i PS NEXT w dwóch kierunkach,
  - ACR-F i PS ACR-F w dwóch kierunkach,
  - ACR-N i PS ACR-N w dwóch kierunkach,
  - RL w dwóch kierunkach,

### 8.2 Pomiary okablowania światłowodowego

- Tłumienie światłowodowego toru transmisyjnego ma być wyznaczone za pomocą miernika OLTS a dodatkowo zaleca się wykonanie pomiarów OTDR,
- Przy pomiarze OTDR należy użyć rozbiegówki oraz dobiegówki w celu określenia jakości wszystkich złączy,
- W przypadku pomiaru OLTS należy wykorzystać metodę pomiarową z 1 kablem referencyjnym (Encircled Flux – dla MM),
- Kompletny pomiar każdego dwupłaskowego toru transmisyjnego wykonanego OLTS i/lub OTDR powinien być przeprowadzony w dwie strony w dwóch oknach transmisyjnych dla dwóch włókien:
  - od punktu A do punktu B w oknie 850nm i 1300nm (MM)
  - od punktu B do punktu A w oknie 850nm i 1300nm (MM)

### 8.3 Zawartość dokumentacji powykonawczej

Po zakończeniu prac instalatorskich należy wykonać i przekazać Użytkownikowi końcowemu dokumentację powykonawczą, która ma zawierać:

- Raporty z pomiarów dynamicznych okablowania,
- Rzeczywiste trasy prowadzenia kabli z lokalizacją przebiegów przez ściany, podłogi, itp.
- Rysunki elewacji szaf z oznaczeniami poszczególnych szaf, paneli krosowych i portów,
- Rzuty z naniesionymi gniazdami. Uwagi końcowe

Trasy prowadzenia okablowania poziomego i pionowego zostały skoordynowane z istniejącymi i wykonywanymi instalacjami w budynku m.in. dedykowaną oraz ogólną instalacją elektryczną, instalacją centralnego ogrzewania, wody, kanalizacji, itp. Jeżeli w trakcie realizacji nastąpią zmiany prowadzenia tras instalacji okablowania lub wystąpią konflikty z innymi instalacjami, należy ustalić poprawione rozprowadzenie tras kablowych w porozumieniu z Projektantem.

Dedykowaną dla okablowania instalację elektryczną należy wykonać zgodnie z obowiązującymi normami i przepisami. Należy uziemić zgodnie obowiązującymi przepisami wszystkie metalowe korytka, drabinki kablowe, szafy kablowe wraz z osprzętem oraz inne urządzenia sieciowe, które zgodnie z instrukcją ich montażu tego wymagają.

Wszystkie materiały wprowadzone do robót muszą być nowe, nieużywane, najnowszych aktualnych wzorów.

## **9 Oświadczenie projektanta i sprawdzającego**

### **Oświadczenie projektanta**

Projektant oświadcza, że niniejszy projekt wykonawczy wykonany jest zgodnie z obowiązującymi przepisami oraz zasadami wiedzy technicznej, a także wytycznymi.

.....

Podpis projektanta

### **Oświadczenie sprawdzającego**

Projektant oświadcza, że niniejszy projekt wykonawczy wykonany jest zgodnie z obowiązującymi przepisami oraz zasadami wiedzy technicznej, a także wytycznymi.

.....

Podpis projektanta

RZUT PIWNICY  
INWENTARYZACJA  
SKALA 1:100

LEGENDA

- Kabel F/FTP kat.6A, 4 pary 23AWG, LSZH  
Kabel OM3 12x50/125/250µm, luznia tuba, 2w, ULSZH  
Kabel U/UTP, 100-parowy kat.3

PL1 – 2x Gniazdo ekranowane 2x RJ45 kat.6a, uchwył 45x45

PL2 – Gniazdo ekranowane 2xRJ45 kat.6a, uchwył 45x45, WFI  
Gniazdo ekranowane 2xRJ45 kat.6a, uchwył 45x45, CCTV

PL3 – Gniazdo ekranowane 1xRJ45 kat.6a, uchwył 45x45, KD

Oznaczenie gniazd (szafa/panel/numer portu)

Główny Punkt Dystrybucyjny – szafa dystrybucyjna 42U

Oznaczenie gniazd (szafa/panel/numer portu)

Piętrowy Punkt Dystrybucyjny – szafa dystrybucyjna 42U

Szczelki kablowe

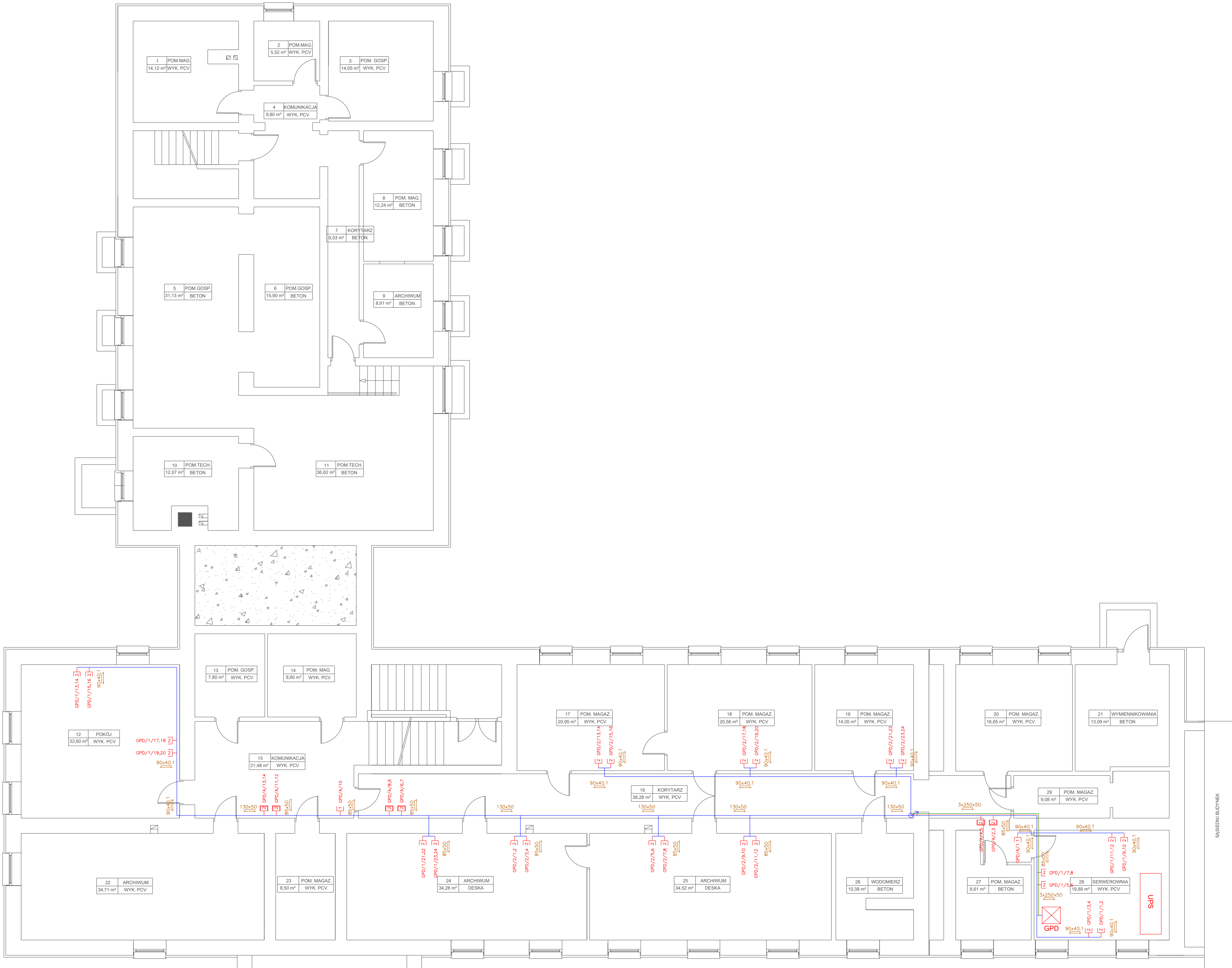
Kanał kablowy dzielony 90x40,1


Kanał kablowy dzielony 85x50

Kanał kablowy dzielony 100x50

Kanał kablowy dzielony 130x50

Kanał kablowy dzielony 250x50



LANSTER Sp. z o. o. – dział projektowy ul. Racławicka 58, 30-017 Kraków, tel: (012) 638 16 66					
OBIEKT	Gmina Proszowice, 32-100 Proszowice, ul. 3 Maja 72				
NAZWA RYSUNKU	Rzut piwnica – instalacja teletechniczna				Branża: Teletechniczna Skala: 1:100
FUNKCJA	IMIĘ I NAZWISKO	UPRAWNIENIA	PODPIS	DATA	Nr rysunku:  T-01
Projektował:	Janusz Wojtyła	Nr upr 0349/97/U		07.2019	
Sprawił:	Eugeniusz Chuderski	Nr upr 1628/99/U		07.2019	



## INWENTARYZACJA

LEGENDA

- Kabel F/UTP kol.6A, 4 pary 23AWG, LSZH
- Kabel OM3 12/50/125/250um, luźna budo. zeł. USLSZH
- Kabel U/UTP, 100-parowy kol.3

PL1 – 2x Gniazdo ekranowane 2x RJ45 kol.6A, uchwyt 45x45

PL2 – Gniazdo ekranowane 2x RJ45 kol.6A, uchwyt 45x45, WFI  
Gniazdo ekranowane 2x RJ45 kol.6A, uchwyt 45x45, CCTV

PL3 – Gniazdo ekranowane 1x RJ45 kol.6A, uchwyt 45x45, KD

Oznaczenie gniazd (szafa/pole/numer portu)

PRD/P1/1/1

  
PRD  
40.800-000

Oznaczenie gniazd (szafa/pole/numer portu)


PRD/P1/1/1

  
PRD  
40.800-000

Piętrowy Punkt Dystrybucyjny – szafa dystrybucyjna 42U

  
PP  
40.800-000

Szacht kablowy

  
CT  
40.800-000

Kanat kablowy dzielony 90x40,1

  
CT  
40.800-000

Kanat kablowy dzielony 85x50

  
CT  
40.800-000

Kanat kablowy dzielony 100x50

  
CT  
40.800-000

Kanat kablowy dzielony 130x50

  
CT  
40.800-000

Kanat kablowy dzielony 250x50


LANSTER sp. z o. o. – dział projektowy ul. Racławicka 58, 30-017 Kraków, tel: (012) 638 16 66				
OBIEKT			Branża: Teletechniczna Skala:	
Gmina Proszowice, 32-100 Proszowice, ul. 3 Maja 72			1:100	
NAZWA RYSUNKU			Nr rysunku:  T-02	
Rzut parteru – instalacja teletechniczna				
FUNKCJA	IMIĘ I NAZWISKO	UPRAWNIENIA	DATA	
Projektował:	Janusz Wojdyła	Nr upr 0349/97/U	07.2019	
Sprawdził:	Eugeniusz Chuderski	Nr upr 1628/99/U	07.2019	

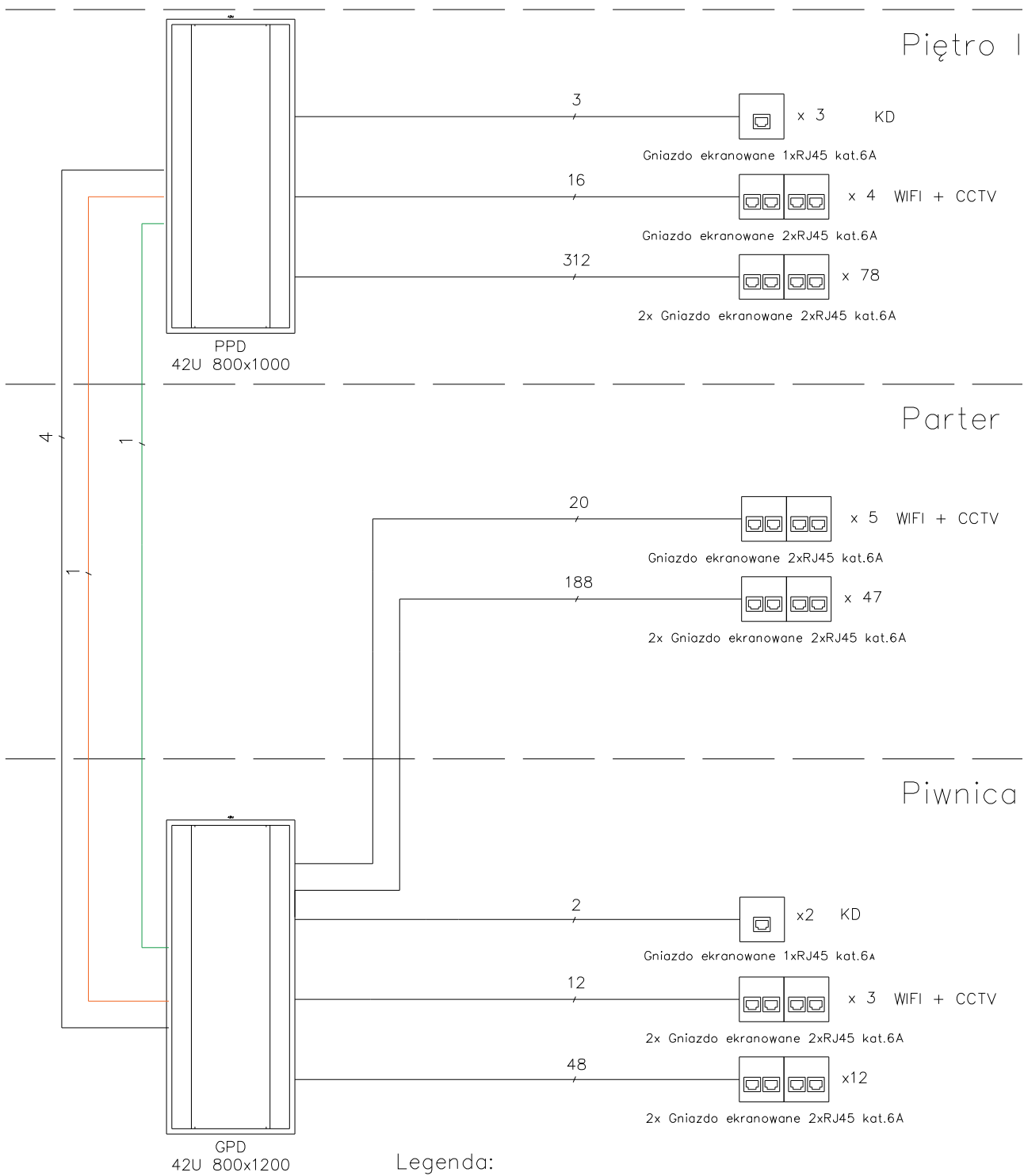



RZUT I PIĘTRA  
INWENTARYZACJA  
SKALA 1:100

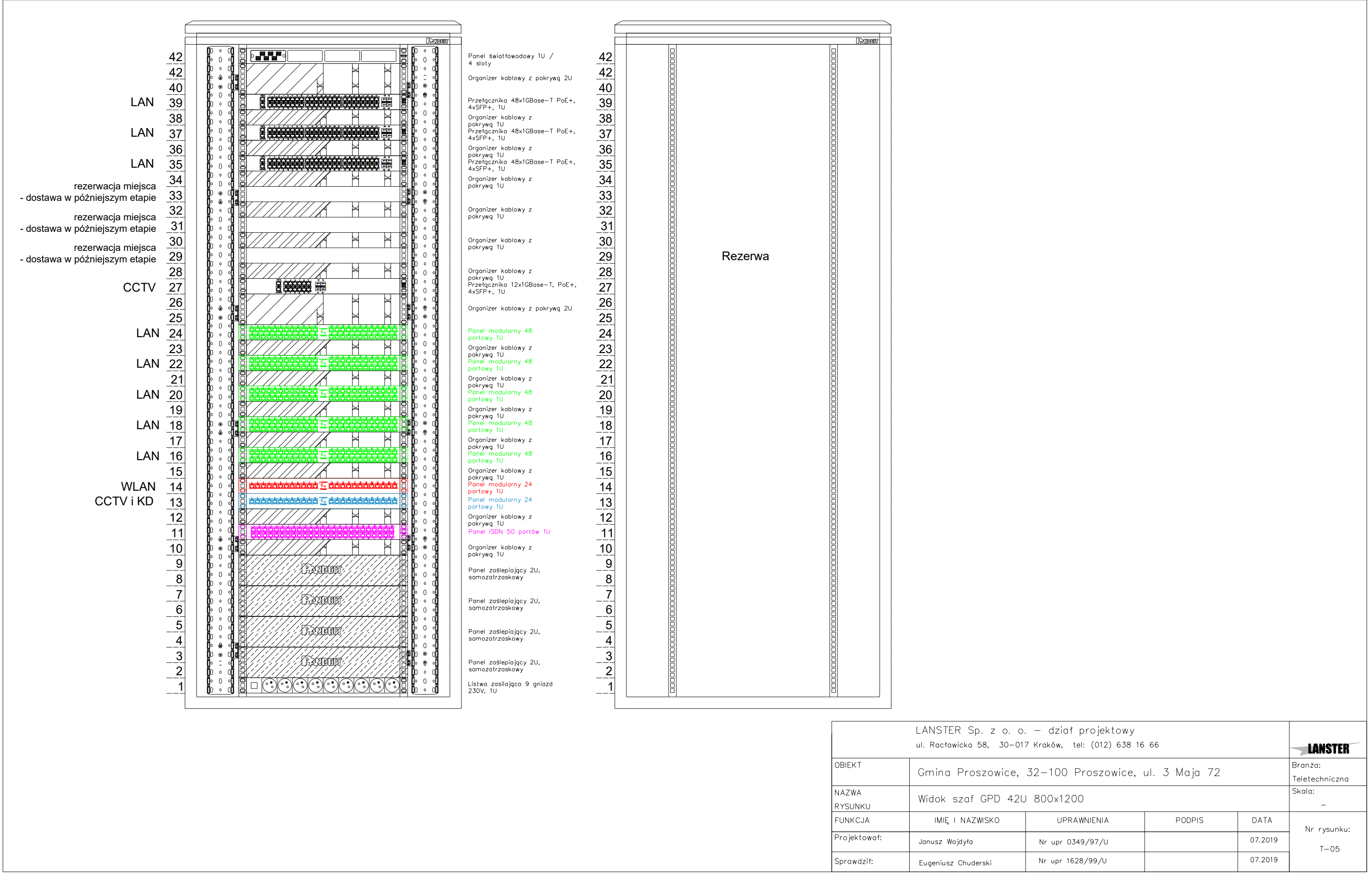
LEGENDA

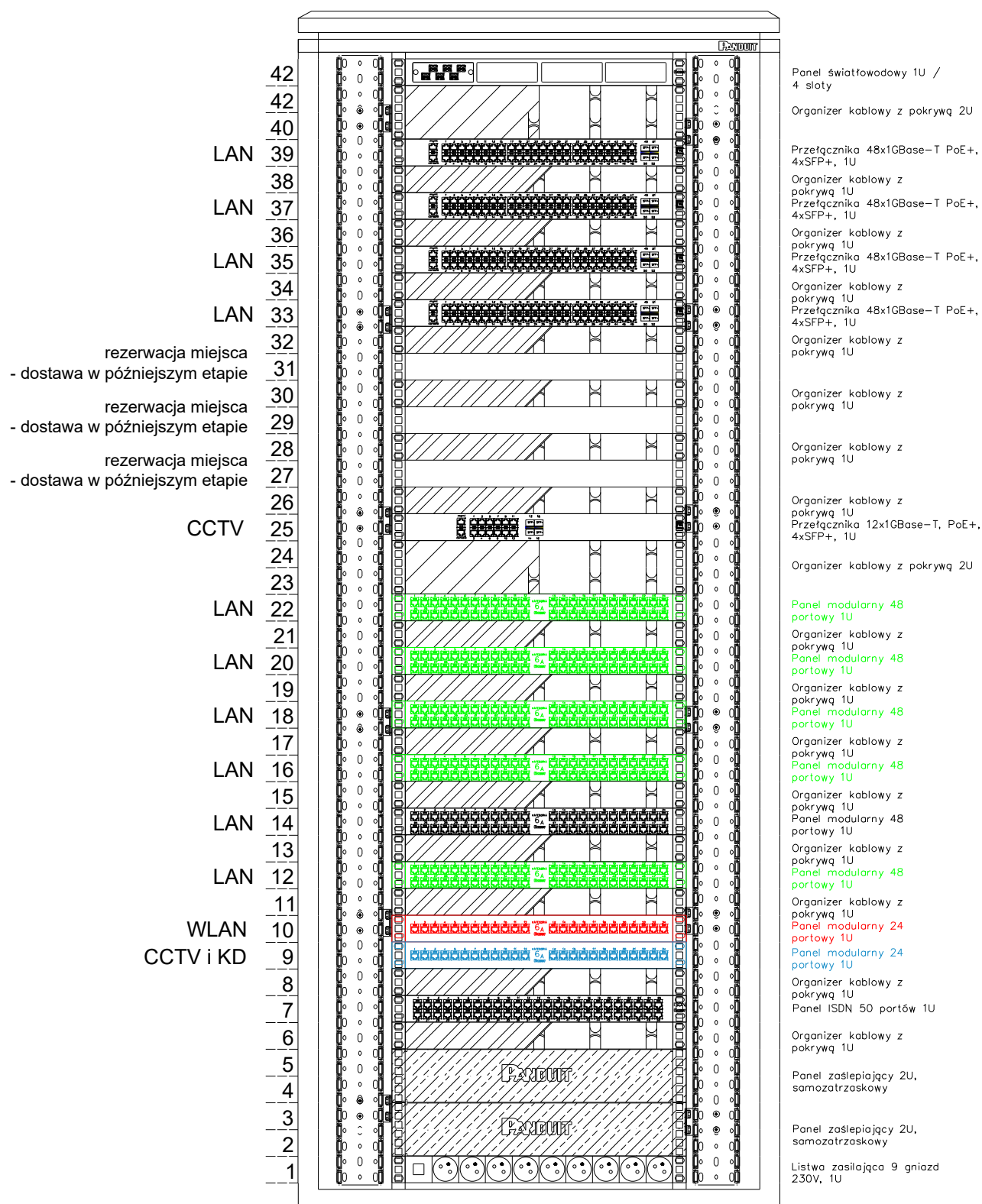
- Kabel F/UTP kat.6A, 4 pary 23AWG, LSZH
- Kabel OM3 12x50/125/250um, luzna tuba, 2H, ULSDH
- Kabel U/UTP, 100-parowy kat.3
- PL1 – 2x Gniazdo ekranowane 2xRJ45 kat.6u, uchwył 45x45
- PL2 – Gniazdo ekranowane 2xRJ45 kat.6u, uchwył 45x45, WFI
- PL3 – Gniazdo ekranowane 1xRJ45 kat.6u, uchwył 45x45, WD
- Oznaczenie gniazd (szafa/panel/numer portu)
- Ołfenny Punkt Dystrybucyjny – szafa dystrybucyjna 42U
- Oznaczenie gniazd (szafa/panel/numer portu)
- Piętrowy Punkt Dystrybucyjny – szafa dystrybucyjna 42U
- Szczelki kablowe
- Kanał kablowy dzielony 90x40.1
- Kanał kablowy dzielony 85x50
- Kanał kablowy dzielony 100x50
- Kanał kablowy dzielony 130x50
- Kanał kablowy dzielony 250x50


LANSTER Sp. z o. o. – dział projektowy ul. Racławicka 58, 30–017 Kraków, tel: (012) 638 16 66					
OBIEKT	Gmina Proszowice, 32–100 Proszowice, ul. 3 Maja 72				
NAZWA RYSUNKU	Rzut I piętra – instalacja teletechniczna				Skala: 1:100
FUNKCJA	IMIĘ I NAZWISKO	UPRAWNIENIA	PODPIS	DATA	Nr rysunku: T–03
Projektował:	Janusz Wojtyła	Nr upr 0349/97/U		07.2019	
Sprawdził:	Eugeniusz Chuderski	Nr upr 1628/99/U		07.2019	



LANSTER Sp. z o. o. – dział projektowy ul. Racławicka 58, 30–017 Kraków, tel: (012) 638 16 66					
OBIEKT	Gmina Proszowice, 32–100 Proszowice, ul. 3 Maja 72				
NAZWA RYSUNKU	Schemat ideowy okablowania				Branża: Teletechniczna
FUNKCJA	IMIĘ I NAZWISKO	UPRAWNIENIA	PODPIS	DATA	Skala: –
Projektował:	Janusz Wojdyła	Nr upr 0349/97/U		07.2019	Nr rysunku:  T–04
Sprawdził:	Eugeniusz Chuderski	Nr upr 1628/99/U		07.2019	





LANSTER Sp. z o. o. – dział projektowy ul. Racławicka 58, 30–017 Kraków, tel: (012) 638 16 66					
OBIEKT	Gmina Proszowice, 32–100 Proszowice, ul. 3 Maja 72				
NAZWA RYSUNKU	Widok szafy PPD 42U 800x1000				Branża: Teletechniczna
FUNKCJA	IMIĘ I NAZWISKO	UPRAWNIENIA	PODPIS	DATA	Skala: –
Projektował:	Janusz Wojdyła	Nr upr 0349/97/U		07.2019	Nr rysunku:  T–06
Sprawdził:	Eugeniusz Chuderski	Nr upr 1628/99/U		07.2019	