PROGRAM FUNKCJONALNO-UŻYTKOWY (PFU)

Modernizacja sieci LAN w Urzędzie Gminy Milicz

w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina”

Zamawiający	**Gmina Milicz**
Adres	**Trzebnicka 2,56-300 Milicz**
Wykonawca	**MOB.IN Grzegorz Gawroński** **ul. Droga Leśna 51/34 ,64-600 Oborniki**
Opracowanie	**Grzegorz Gawroński**

1. Cześć Opisowa

1.1 Opis ogólny przedmiotu zamówienia

Wykonanie modernizacji i rozbudowy wewnętrznej sieci LAN jest częścią realizowanego projektu pn. Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina" poprzez:

- Podwyższenia parametrów transmisyjnych wyeksploatowanej istniejącej sieci teleinformatycznej;
- rozbudowy sieci o dodatkowe punkty logiczne (PL);
- budowy dedykowanej instalacji sieci zasilającej dla potrzeb węzłów sieci;
- modernizacji węzłów sieci LAN;
- optymalizacji rozmieszczenia Punktów Logicznych (PL);

Modernizacja sieci LAN będzie dotyczyła fizycznej rozbudowy infrastruktury kablowej obejmującej wykonanie nowych przyłączy logicznych w pomieszczeniach urzędu oraz dostawę urządzeń aktywnych. W ramach zadania należy wykonać 186 nowych linii sieci LAN. Struktura sieci będzie sprowadzona do topologii gwiazdy-drzewa ograniczonej wyłącznie do węzłów dystrybucyjnych, bez kolejnych rozgałęzień. Zostaną wymienione przełączniki sieciowe, przez co cała struktura będzie zarządzalna oraz pozwoli na znaczące podniesienie poziomu bezpieczeństwa i wydajności sieci.
Materiał zawarty w niniejszym PFU jest wytyczną dla wykonawcy do wykonania kompleksowej realizacji zadania. Zawiera niezbędne informacje do przygotowania oferty przetargowej, a w późniejszym etapie do wykonania zadania.

Zamówienie musi spełniać wymogi określone w ustawie z dnia 7 lipca 1994 r. Prawo budowlane, Rozporządzenia Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 25 kwietnia 2012 r. w sprawie szczegółowego zakresu i formy projektu budowlanego oraz ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych.

1.2 Zakres rzeczowy robót

W ramach realizacji należy wykonać usługę i dostawy zgodnie z poniższym zestawieniem. Rozwiązania i usługi muszą być zgodne z minimalnymi wymaganiami zawartymi w niniejszym dokumencie.

- układanie kabli miedzianych w nowych trasach;
- instalacja punktów logicznych;
- montaż paneli krosowych w punktach dystrybucyjnych
- dostarczenie i montaż do szafy telekomunikacyjnej paneli krosowych;
- dostosowanie ilości paneli do liczby instalowanych punktów sieci LAN;

- zakończenie linków miedzianych złączami RJ45 kat. 6A lub wyższej;
- wykonanie pomiaru linków miedzianych;
- dostawa i montaż patchcordów miedzianych kat. 6A lub wyższej;
- wykonanie dokumentacji powykonawczej.

1.3 Stan obecny sieci LAN

Obecnie urząd posiada sieć komputerową LAN zbudowaną w większości w oparciu o kabel kat.5. Główny punkt dystrybucyjny sieci znajduje się w pomieszczeniu serwerowni, z którego poprowadzone jest okablowanie na terenie urzędu. Budynek Urzędu Miasta i Gminy znajduję się pod opieką konserwatora zabytków.

1.4 Ogólne właściwości funkcjonalno – użytkowe

W stosunku do aktualnego rozwiązania planowana modernizacja sieci teleinformatycznej LAN poprawi organizację sieci oraz spowoduje zwiększenie ilości linii i gniazd sieci LAN oraz ułatwi zarządzanie. Stanowiska pracy będą kompleksowo podłączane do punktów logicznych (PL). Sieć LAN będzie posiadła parametry transmisyjne nie gorsze od dotychczasowej. Wydajność sieci ulegnie znacznej poprawie dzięki zastosowaniu urządzeń o znacznie wyższych parametrach od parametrów istniejących urządzeń. Urządzenia muszą zagwarantować transmisję z wydajnością 10Gb/s pomiędzy punktami dystrybucyjnymi, wydajność pomiędzy urządzeniami w stosie minimum 40Gb/s oraz transmisję pomiędzy przełącznikiem a urządzeniem końcowym minimum 1Gb/s.

1.5 Prowadzenie robót

Wszelkie prace budowlane powinny odbywać się zgodnie z przepisami prawa, w szczególności Prawem budowlanym, Prawem telekomunikacyjnym, Rozporządzeniem Ministra Infrastruktury z dnia 26 października 2005 r. w sprawie warunków technicznych, jakim powinny odpowiadać telekomunikacyjne obiekty budowlane i ich usytuowanie, Polskimi Normami, Normami Europejskimi oraz stosownymi Normami Branżowymi. Zamawiający wymaga, aby wszelkie prace wykonywane były z zachowaniem ciągłości pracy Urzędu Miejskiego i nie powodowały utrudnień w codziennym jego funkcjonowaniu, a także zapewniały bezpieczeństwo pracowników Urzędu oraz Petentów.

1.6 Odbiór placu budowy

Przed rozpoczęciem modernizacji robót dotyczących modernizacji instalacji okablowania sieci LAN wraz z dedykowaną instalacją zasilającą, wykonawca powinien zapoznać się z obiektem urzędu, w którym prowadzone będą roboty, istniejącą instalacją sieci komputerowej LAN i instalacją zasilania elektrycznego.

1.7 Koordynacja robót z innymi robotami

Koordynacja robót instalacyjno-montażowych poszczególnych rodzajów powinna być dokonana we wszystkich fazach procesu robót budowlanych. Koordynacją należy objąć projekt organizacji budowy, szczegółowy harmonogram instalacji okablowania strukturalnego wraz z dedykowaną instalacją zasilania elektrycznego oraz pomocnicze roboty ogólnobudowlane związane modernizacją okablowania strukturalnego sieci LAN i serwerowni.

2. Wymagania Zamawiającego.

2.1 Wymagania podstawowe

Pracownicy biorący udział w realizacji zamówienia muszą posiadać aktualne i stosowne do zakresu wykonywanych prac uprawnienia i badania, które powinny być przedstawione Zamawiającemu przed rozpoczęciem prac.

Wszystkie stosowane materiały i urządzenia muszą być fabrycznie nowe i dobrej jakości, nie używane wcześniej w żadnych projektach, nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy, a także muszą dokładnie odpowiadać warunkom niezbędnym do prawidłowego wykonania powierzonych robot oraz do poprawnego funkcjonowania całej instalacji.

Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.

Stosowane materiały i urządzenia muszą posiadać wymagane deklaracje zgodności lub certyfikaty dopuszczające do stosowania ich w budownictwie.

Wykonawca zobowiązany jest do pozostawienia pomieszczeń w których będą wykonywane prace w stanie takim jaki zastał przed przystąpieniem do prac.

2.2 Wymagania w zakresie modernizacji sieci LAN

- **Wymagania ogólne dla sieci komputerowej:**

W ramach modernizacji istniejącej sieci LAN należy wykonać miedziane okablowanie sieci LAN w oparciu o kabel ekranowany typu skrętka kategorii 6 A wraz z dedykowaną elektryczną instalacją zasilającą. Należy rozbudować istniejącą sieć LAN o około 186 linii sieci LAN zakończonych gniazdami RJ45 pogrupowanymi w punkty logiczne (PL) 1xRJ45, 2xRJ45 3xRJ45. Wstępną lokalizację oraz ilość gniazd RJ45 w poszczególnych pomieszczeniach oznaczono czerwonym znakiem (znak = 1 x RJ45) na schemacie rozmieszczenia punktów dostępowych LAN stanowiący załącznik nr 1 do PFU. Szczegółową docelową lokalizację PL w pomieszczeniach należy uzgodnić z Zamawiającym. Cały system okablowania sieci ma być zgodny z obowiązującą specyfikacją Kat.6A. System okablowania strukturalnego musi być wykonany zgodnie z przygotowaną dokumentacją wykonawczą, wszelkie zmiany i odstępstwa muszą być pisemnie

zatwierdzone przez uprawnionego przedstawiciela Zamawiającego i uwzględnione w dokumentacji powykonawczej. W celu uzyskania maksymalnej kompatybilności wszystkich elementów toru transmisyjnego oraz możliwość uzyskania jednolitej gwarancji systemowej wszystkie elementy okablowania muszą pochodzić od jednego producenta. Składniki systemu muszą być zainstalowane przez Certyfikowanego Instalatora oferowanego systemu okablowania.

Wymagana jest jednolita 25-letnia bezpłatna gwarancja na system od producenta oferowanego systemu okablowania strukturalnego. 25-letnia gwarancja powinna obejmować tor transmisyjny od gniazda abonenckiego do gniazda RJ45 w panelu w szafie. 25 letnia gwarancja będzie ważna, gdy instalacja została wykonana zgodnie z międzynarodowymi standardami branżowymi dotyczące budowy sieci teleinformatycznych jak i z polskimi, a w szczególności PN-EN 50174-1, PN-EN 50346, PN-EN 61935-1. Zamawiający wymaga certyfikatu gwarancyjnego okablowania udzielonego bezpośrednio Użytkownikowi końcowemu i stanowiącego 25-letnie zobowiązanie gwarancyjne producenta w zakresie dotrzymania parametrów wydajnościowych, jakościowych, funkcjonalnych i użytkowych wszystkich elementów toru oddzielnie i całego systemu okablowania. Poprawność wykonania pod względem transmisji sygnałowej musi zostać potwierdzona odpowiednimi protokołami pomiarowymi. Miernik wykorzystywany do pomiarów powinien spełniać wymagania stawiane urządzeniom IV poziomu dokładności (Level IV wg in IEC 61935-1/Ed. 3 lub równoważnej) i posiadać aktualną kalibrację. Całość okablowania (dotyczy również kabli krosowych) musi posiadać izolacje wykonane z materiału nie wydzielającego podczas pożaru szkodliwych gazów (LS0H lub LSZH lub LSHF).

- **Kabel transmisyjny**

Kabel musi być ekranowany i spełniać wymagania minimum kategorii 6 A w paśmie do 500MHz wg ISO/IEC 11801 lub normy równoważnej, z żyłami miedzianymi jednodrutowymi o średnicy 23AWG.Promienie gięcia muszą być zgodnie z normą producenta oraz powinny być zakończone w sposób trwały na8 -pozycyjnym złączu. Kable transmisyjne należy zakończyć w szafie RACK na 19” panelach rozdzielczych.

- **Punkt dostępowy LAN**

Punkty dostępowe sieci LAN należy wykonać zgodnie z zatwierdzoną dokumentacją projektową uwzględniającą minimalne wymagania dla sieci określone przez Zamawiającego w niniejszym dokumencie. Punkt dostępowy w postaci gniazda teleinformatycznego RJ45 w standardzie Mosaic 45 minimum kategoria 6A należy zamontować w puszce p/t na płycie czołowej zapewniającej zgodne z normą producenta promień gięcia kabla w puszce. Kategoria gniazda musi być zgodna z kategorią użytego kabla. Gniazda muszą być wyposażone w złącza szczelinowe IDC z sekwencją 568A/B. Gniazdo RJ45 musi posiadać przesłonę przeciwkurzową wbudowaną w moduł. Przesłona powinna się chować do środka podczas wpinania wtyku RJ45 w gniazdo. Moduły zainstalowane w PL musza zostać ponumerowane w sposób trwały i widoczny, według następującego schematu: PP- NN gdzie PP to kolejny numer panelu w szafie dystrybucyjnej, NN numer gniazda w danym panelu.

- **Panele rozdzielcze**

W ramach zamówienia należy dostarczyć i zainstalować odpowiednią ilość paneli rozdzielczych 19” przeznaczonych do montażu w szafie RACK. Panel rozdzielczy minimum kategorii 6 A, 24 lub 48 portowy w zależności od potrzeb danego węzła. Panele 19” do podłączania kabli w węzłach sieci muszą być wykonane z gniazdami RJ45 na płytkach PCB, celem lepszej eliminacji przesłuchów pomiędzy gniazdami. Panel musi posiadać uniwersalne złącza szczelinowe IDC z sekwencją 568A/B. Panel musi być metalowy, malowany proszkowo. Nie dopuszcza się paneli z tworzyw sztucznych. Panel musi posiadać miejsce do wielokrotnego oznaczania portów, w celu umożliwienia łatwego dokonywania zmian opisów. Możliwość zastosowania dla każdego oddzielnego portu RJ45 dodatkowego oznaczenia sugerującego przeznaczenie portu, itp. poprzez wpięcie kolorowej ikony posiadającej piktogram komputera (usługa LAN), telefonu (usługa Voice), oraz bez rysunku. Panel musi posiadać półkę służąca do przyłączania terminowanych kabli za pomocą krawatek dzięki czemu kable nie obciążają złącz szczelinowych oraz uniemożliwia się przypadkowe wyrwanie kabla. Panel musi być wyposażona w moduły RJ45 z przesłoną przeciwkurzową, chowaną do środka podczas wpinania wtyku RJ45 w gniazdo. Pomiędzy panelami rozdzielczymi należy umieścić 19” panele porządkujące o wysokości 1U.

- **Panele światłowodowe**

Panel musi być metalowy, malowany proszkowo. Nie dopuszcza się paneli z tworzyw sztucznych. Panel powinien składać się korpusu panela tj. obudowy montowanej w ramie 19” oraz wymiennych paneli przednich (płyt czołowych) wpinanych w korpus panela. Panel musi istnieć możliwość wymiany płyty czołowej na inną (np. o większej pojemności) bez konieczności deinstalacji zainstalowanych kabli i ponownego terminowania złącz światłowodowych. Panel powinien posiadać konstrukcję wysuwaną, tj. pozwalająca na wysunięcie płyty czołowej oraz ustawienie pod kątem umożliwiając łatwy dostęp do zapasu włókna, złącz światłowodowych i kasety spawów. Szuflada powinna posiadać blokadę zabezpieczającą przed niepożądanym wysunięciem np. w momencie wypinania kabla krosowego.

- **Przewody krosowe**

Dla nowych punktów sieci LAN, wykonawca zapewni w ramach wykonania usługi odpowiednią ilość kabli krosowych (z zachowaniem kat.6A) dla realizacji połączeń jednostek komputerowych z pobudowanym torem logicznym (długość zależna od rozmieszczenia stanowisk komputerowych od 3m do 5m) oraz niezbędnych do połączeń aktywnych i pasywnych elementów sieci w szafie dystrybucyjnej (od 0,5m do 2 m).

- **Główny punkt dystrybucyjny**

Główny punkt dystrybucyjny (GPD) zostanie zlokalizowany w serwerowni. GPD należy wyposażyć w szafę stojącą typu RACK 19” o wymiarach 42U 800x1000 na cokole z płytą dolną otworowaną umożliwiającą doprowadzenie okablowania. Elementy szafy muszą być wykonane z blachy stalowej malowanej proszkowo. Szkielet stalowy malowany proszkowo lub ocynkowany. Drzwi przednie stalowe perforowane zamykane na zamek. Drzwi tylne stalowe uchylne z zamkiem. Drzwi

boczne demontowane na zatrzaskach z możliwością montażu zamka. Szafa musi być wyposażona w minimum dwie półki, dwie listwy zasilające z minimum 6 gniazdami w obudowie aluminiowej, panel wentylacyjny z czterema wentylatorami, panel rozdzielczy 24 portowy wyposażony w moduły RJ45 oraz panel światłowodowy.

- **Pośrednie punkty dystrybucyjne**

Pośrednie punkty dystrybucyjne zostaną zlokalizowane na parterze oraz 2 piętrze budynku urzędu. Każdy punkt należy wyposażyć w szafę wisząca min 12 U. Do każdego punktu należy doprowadzić zasilanie elektryczne. Wszystkie gniazda energetyczne służące do zasilania węzłów sieci muszą posiadać zabezpieczenie uniemożliwiające włączenie innych niż dedykowane urządzenia, aby uniemożliwić podłączenia dowolnych urządzeń elektrycznych, a tym samym wprowadzić podniesienie bezpieczeństwa użytkowania.

- **Okablowanie światłowodowe**

Punkty GPD z punktami PPD należy połączyć z wykorzystaniem kabli światłowodowych jednomodowych min 6 -cio włóknowych.

2.3 Urządzenia sieciowe

Parametry minimalne przełącznik sieciowy – 5 szt.

- Przepustowość: 176 Gbps
- Szybkość przesyłania w Mpps (pakiety 64 bajtowe): 120
- Porty 10/100/1000: 48
- Porty uplink: 4 SFP+
- Porty obsługujące PoE+ (802.3af/at): 48
- Port konsoli: tak
- Port USB: tak
- Port zarządzania pozapasmowego: tak
- Wielkość tablicy MAC: 16K
- Wielkość pamięci flash: 128 MB
- DRAM: 512 MB
- VLANy: 4 tys.
- Sieci VLAN oparte na portach: 4 tys.
- Kolejki priorytetowe QoS: 8
- PVRST: 32
- Przychodzące/wychodzące listy ACL: 128
- Wpisy ARP: 512
- Statyczne wpisy ARP: 512

- Trasy statyczne: 64
- Routing dynamiczny: 512
- Policy Base Automation: tak
- QoS:
  - Mapowanie ACL i oznaczanie ToS/DSCP
  - Mapowanie ACL dla 802.1p
  - Mapowanie ACL do kolejek priorytetowych
  - Obsługa DiffServ
  - Zarządzanie kolejką priorytetową przy użyciu metod Wieght Round Robin (WRR), Strict Priority (SP) oraz połączenie WRR i SP
- Zarządzanie ruchem:
  - Zasady ograniczania prędkości połączeń przychodzących oparte na ACL
  - Ograniczenie prędkości transmisji, multicast i uknown unicast
  - Ograniczenie prędkości przychodzących na port
  - Ograniczenie szybkości połączeń wychodzących na port/kolejkę
- Bezpieczeństwo:
  - Uwierzytelnianie 802.1x
  - Uwierzytelnianie MAC
  - DHCP snooping
  - Uwierzytelnianie/autoryzacja poprzez RADIUS
  - Secure shell
  - Bezpieczna kopia (SCP)
  - Lokalna nazwa użytkownika/hasło
- Zestaw funkcji warstwy 2:
  - 802.1d
  - Uwierzytelnianie 802.1x
  - Auto MDI/MDIX
  - BPDU Guard, Root Guard
  - IGMP Snooping v1/v2/v3
  - LLDP/LLDP MED
  - IGMP Proxy
  - Statyczny MAC
  - Port Mirroring: port based, ACL based, VLAN based
  - Izolacja portów/Privet VLAN Edge
  - Link Aggregation Group (Static/LACP)
  - Rate Limiting/Storm Control
  - Jumbo frame: 9K
  - DHCP Snooping
  - Filtrowanie BPDU
  - Ochrona przed atakami typu DoS
  - Ping/TraceRoute/ICMPv6
- Zestaw funkcji warstwy 3:
  - Routing pomiędzy VLAN
  - Statyczne ARP
  - Trasy statyczne

  - Przekazywanie DHCP
  - Routing dynamiczny: RIPv1/v2, OSFPv2
  - Redystrybucja tras
- Zarządzenia:
  - Kontroler chmurowy
  - Standardowy interfejs wiersza poleceń (CLI)
  - DHCP client
  - Wbudowane sieciowe zarządzenia (HTTP/HTTPS)
  - Wbudowany serwer DHCP
  - SSH/SSHv2
  - SNMP v1/v2/v3
  - Przekazywanie DHCP
  - Simpe Network Time Protocol (SNTP)
  - Lokalny/zdalny system logowania
  - TFTP/SFTP
  - Telnet client/server
  - Zarządzanie po IPv6
- Switching:
  - Core Switching Features:
    - IEEE 802.1ab – Link Layer Discovery Protocol (LLDP)
    - IEEE 802.1D – Spanning tree compatibility
    - IEEE 802.1p – Ethernet priority with user provisioning and mapping
    - IEEE 802.1s – Multiple spanning tree compatibility
    - IEEE 802.1Q – Virtual LANs with port-based VLANs
    - IEEE 802.1X – port-base authentication
  - VLAN Support:
    - IEEE 802.1W – Rapid spanning tree compatibility
    - IEEE 802.3 – 10BASE-T
    - IEEE 802.3u – 100BASE-T
    - IEEE 802.3ab – 1000BASE-T
    - IEEE 802.3ac – VLAN tagging
    - IEEE 802.3ad- Link aggregation
    - IEEE 802.3x – Flow control
- Parametry fizyczne:
  - Zasilanie: 100-240 VAC
  - Maksymalna moc przełącznika: 39,24 W
  - Waga: 5,4 kg
  - Szybkość CPU: 800 MHz
  - Budżet mocy PoE+: 400W
  - Budżet mocy PoE per port: 30W
  - Możliwość montażu w szafie: tak, 1U
  - Zestaw do montażu w szafie rack: tak
  - Wewnętrzne wentylatory: 2
  - Zakres temperatur pracy: od 0°C do 50°C

Parametry minimalne urządzenia do backupu:

Parametr	Charakterystyka (wymagania minimalne)
Procesor	Intel® Xeon® E-2334 4C 8T o taktowaniu 3,4 GHz zwiększanym do 4,8 GHz
Architektura procesora	64-bit x86
Pamięć RAM	Nie mniej niż 16 GB DDR4 ECC
Pamięć RAM liczba slotów	Minimum 4 sloty
Pamięć RAM - możliwość rozszerzenia	128 GB (4 x 32 GB)
Pamięć Flash	Nie mniej niż 4GB
Liczba zatok na dyski twarde	18 (12 x 3,5-calowych SATA + 6 x 2,5-calowych SATA)
Obsługiwane dyski twarde	3.5" SATA oraz 2.5" SATA / SSD SATA
Dostarczone dyski twarde	4 dyski 4TB klasy NAS SSD / gwarantowana kompatybilność producenta
Pojemność dysków twardych jakie można stosować	Do 14 TB
Możliwość podłączenia moduły rozszerzającego	Tak
Porty LAN	2 (2,5G/1G/100M), 2 x 10GBASE-T (10G/5G/2,5G/1G/100M)
Diody LED	HDD 1–24, stan, LAN, stan gniazda rozszerzenia pamięci masowej
Porty USB 3.1 GEN 2 (10 Gb/s)	2 gniazda typu C USB 3.1 Gen2 5V/3A 10 Gb/s 4 gniazda typu A USB 3.1 Gen2 5V/1A 10 Gb/s
Przyciski	Reset, Zasilanie
Typ obudowy	RACK, 3-4U
Dopuszczalna temperatura pracy	od 0 do 40˚C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Redundantne 800 W(x2), 100–240 V
Wysyłanie / odbieranie w systemie Windows	min. 1800 (MB/s) / 2300 (MB/s) (przy agregacji 2 łączy 10 Gb/s i transferze pliku 10 GB)
Wysyłanie / odbieranie w systemie Windows (Robocopy) - z wykorzystaniem szyfrowania AES 256bit	min. 1500 (MB/s) / 2200 (MB/s) (przy agregacji 2 łączy 10 Gb/s i transferze pliku 10 GB)
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Możliwość podłączenia karty WLAN na USB	Tak
Łączenie usług z interfejsem	Tak

Szyfrowanie wolumenów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, RAID 0,1, 5,50, 6, 60, 10, 5+Hot Spare, 6+Hot SPare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Globalny Hot Spare, Pula pamięci masowej Mechanizm automatycznego pozycjonowania danych w zależności od częstotliwości wykorzystania SSD over provisioning Funkcjonalność migawek dla woluminów oraz LUN, wraz z możliwością ich replikacji na drugie urządzenie Obsługa SSD cache w trybach read i write
Wbudowana obsługa iSCSI	Multi-LUNs na Target Minimum do 256 LUNs Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników do domeny poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Obsługa uwierzytelniania NTLMv2, Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, serwer Apple Time Machine, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Amazon S3, Amazon Glacier, Microsoft Azure, Google Cloud Storage, Dropbox,
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer baz danych MySQL Serwer kopii zapasowych Serwer multimediów UPnP Serwer wydruku Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu (opcja podłączenia 8 kamer IP w ramach wbudowanj licencji z możliwośćia podłączenia dodatkowych po dokupieniu licencji)
VPN	VPN client / VPN server. Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS

	Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania ręczna Możliwość aktualizacji oprogramowania z powiadomieniem z serwerów producenta Ustawienia: Back up, przywracania, resetowania systemu
Wirtualizacja	możliwość uruchomienia maszyn wirtualnych z systemem Windows, Linux, Unix i Android; import maszyn wirtualnych z systemów VirtualBox, Vmware Workstation; VM clone, VM snapshot; pass-throug dla USB;
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH)
	Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek oraz wbudowane narzędzia wirtualizacji umożliwiającee zarówno obsługę kontenerów Docker/LXC jak i pełnych maszyn wirtualnych
Współpraca z środowiskami wirtualnymi	VMware vSphere, Citrix XenServer, Windows Server 2016, PlugIn dla vSphere, obsługa Vmware VAAI dla iSCSI

Parametry minimalne UTM

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
Wymagania ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie:

	Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: Firewall. Ochrony w warstwie aplikacji. Protokołów routingu dynamicznego.
2. Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS — musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
3. Interfejsy, Dysk, Zasilanie:	1. System realizujący funkcję Firewall musi dysponować minimum: - 10 portami Gigabit Ethernet RJ-45. - 2 gniazdami SFP 1 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802. IQ. 4. System musi być wyposażony w zasilanie AC.
4. Parametry wydajnościowe:	1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http — minimum 700 Mbps.
5. Funkcje Systemu Bezpieczeństwa:	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy StatefulInspection.

	2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware — co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - IntrusionPrevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty — Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Trafficshaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. 12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DOT) oraz DNS over HTTPS (DOH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system
6. Polityki, Firewall	13.2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 14.3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: - Translację jeden do jeden oraz jeden do wielu. - Dedykowany ALG (Application Level Gateway) dlaprotokołu SIP. 15. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 17. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. - Amazon Web Services (AWS). - Microsoft Azure - Google Cloud Platform (GCP). - OpenStack. - VMware NSX.
7. Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: - Wsparcie dla IKE VI oraz v2. - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/CounterMode(GCM). - Obsługa protokołu Diffie-Hellman grup 19 i 20. - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.

	- Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. - Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: - Pracę w trybie Portal gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. -Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
8. Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie powinno zapewniać obsługę: - Routingu statycznego. - Policy Based Routingu. - e Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
9. Funkcje SD-WAN	1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2.Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
10. Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
11. Ochrona przed malware	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji Al wytrenowanego przez laboratoria producenta.
12. Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

	5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DOS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
13. Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
14. Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków — białe/czarne listy dla adresów URL. 5. Funkcja SafeSearch — przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
15 Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. - Haseł dynamicznych (RADIUS, RSA SecurlD) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

16. Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
17. Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Musi istnieć możliwość logowania do serwera SYSLOG.
18.Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall.
19. Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.
20Gwarancja	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości.

21Wsparcie	Wsparcie: W ramach serwisu gwarancyjnego producent musi zapewniać dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
22. Rozszerzone wsparcie serwisowe AHB/SOS	Certyfikat ISO 9001 podmiotu serwisującego.
23. Opisy do wymagań ogólnych	Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Zamawiający wymaga szkolenia w zakresie obsługi zakupionego sprzętu dla wskazanych pracowników urzędu.

2.4 Instalacja i konfiguracja urządzeń

Wykonawca dostarczy aktywny sprzęt sieciowy do lokalizacji, którą jest siedziba Zamawiającego, na własny koszt. Dostarczone urządzenia muszą być zainstalowane w szafach RACK zgodnie z wymaganą konfiguracją węzłów sieci, podłączone, skonfigurowane i uruchomione. Wszystkie elementy niezbędne do instalacji (śruby montażowe, kable, przewody, listwy zasilające, itp.) muszą być zapewnione przez Wykonawcę. Zamawiający wymaga połączenia urządzeń aktywnych przy wykorzystaniu okablowania dostarczonego przez Wykonawcę wraz z urządzeniami. Porty Base-T przełączników dystrybucyjnych muszą być połączone za pomocą kabli krosowych z odpowiednimi gniazdami RJ45 w panelach krosowych sieci LAN. Zamawiający wymaga połączenia węzłów sieci z wykorzystaniem dostarczonych wraz z przełącznikami modułów 10G SFP+ ze złączem typu LC lub równoważnym. W przypadku przełączników agregacyjnych należy wykonać światłowodowe połączenia agregacyjne z przełącznikami rdzeniowymi oraz serwerami i macierzami z wykorzystaniem modułów 10G SFP+ dostarczonych wraz z przełącznikami. W przypadku instalacji w jednym miejscu dwóch lub więcej przełączników, muszą być połączone w stos za pomocą dostarczonego okablowania oraz odpowiednich modułów dostarczonych wraz z przełącznikami, zapewniających transmisję.

Porty Base-T przełączników muszą być połączone za pomocą kabli krosowych z odpowiednimi gniazdami RJ45 w panelach krosowych sieci LAN.

Przełączniki muszą być skonfigurowane zgodnie ze wskazaniami i uzgodnieniami z Zamawiającym na etapie instalacji. Konfiguracja powinna zapewniać minimum 2 podsieci (VLAN) oraz umożliwiać autoryzację IEEE 802.1x.

Wymagana jest konfiguracja urządzeń w zakresie:

- sieci VLAN, adresacji IP, interfejsów VLAN;
- interfejsów fizycznych, funkcjonalności LACP;
- funkcjonalności routingu;

- stackowania przełączników;
- polityk bezpieczeństwa, QoS, mechanizmów STP i ich bezpieczeństwa;
- mechanizmów zarządzania urządzeniami (np. SSH, telnet, SNMP, HTTPS);
- autoryzacji IEEE 802.1x.

Wykonawca przeprowadzi instruktarz dla administratorów sieci Zamawiającego obejmujący minimum w/w zagadnienia związane z konfiguracją i zarządzaniem urządzeniami. Czas trwania instruktarzu musi zapewnić pełną zrozumiałość zagadnień przez wytypowanych przedstawicieli Zamawiającego, potwierdzoną protokołem przeprowadzenia instruktażu.

Po instalacji i konfiguracji sprzętu, wykonawca wykona testy połączeń i wydajności urządzeń. Pozytywny wynik testów będzie podstawą podpisania protokołu odbioru.

2.5 Dokumentacja Powykonawcza

Po zakończeniu robót należy przygotować dokumentację powykonawczą zawierającą co najmniej następujące elementy:

- informacje o inwestorze;
- wykonawcy rozpatrywanej instalacji;
- opis wykonanej instalacji wraz z opisem wybranej technologii;
- rysunki powykonawcze uwzględniające zmiany w wykonaniu prac instalacyjnych dla tras kablowych, szaf i rozdzielni oraz z zaznaczonymi miejscami przejść przez ściany i stropy;
- lista zainstalowanych komponentów: Lp. / Producent – Dostawca / numer katalogowy / nazwa elementu / nr seryjny / ilość;
- schemat połączeń elementów instalacji uwzględniające lokalizację na terenie obiektu, opisy poszczególnych szaf, gniazd, kabli i portów w panelach krosowych oraz zmiany w istniejących opisach;
- schematy instalacji elektrycznej;
- widoki szaf i stojaków w punktach dystrybucyjnych;
- podpisane przez uprawnione osoby protokoły pomiarowe sieci teleinformatycznej i instalacji elektrycznej;
- dokumentację, raporty (w formie tekstowej lub wydruku z konsoli administracyjnej) konfiguracji oraz schematy połączeń zainstalowanych przełączników sieciowych. Dokumentacja musi uwzględniać m.in. adresację urządzeń oraz hasła;

Informacje zawarte w dokumentacji powykonawczej muszą zgadzać się z rzeczywistością.

Dokumentacja powykonawcza musi zostać przygotowana w języku polskim.

Należy dostarczyć 2 egzemplarze dokumentacji powykonawczej w formie papierowej, oraz dokumentację elektroniczną w standardzie PDF i w wersji edytowalnej zapisanej na nośniku CD, lub DVD, ”, nie później niż na 5 dni przed zgłoszeniem gotowości do odbioru końcowego.

3. Wykonanie robót budowlanych

3.1 Zasady wykonania robót

Podczas realizacji robót wykonawca będzie przestrzegać przepisów dotyczących bezpieczeństwa i higieny pracy. W szczególności wykonawca ma obowiązek zadbać, aby personel nie wykonywał pracy w warunkach niebezpiecznych, szkodliwych dla zdrowia oraz niespełniających odpowiednich wymagań sanitarnych. Wykonawca zobowiązany jest do pozostawienia pomieszczeń w których będą wykonywane prace w stanie takim jaki zastał przed przystąpieniem do prac. Wykonawca zobowiązany będzie do wywiezienia odpadów, opakowań, materiałów z rozbiórki na własny koszt oraz ich utylizację zgodnie z przepisami w zakresie ochrony środowiska. Wykonawca zobowiązany będzie do przedłożenia Zamawiającemu dokumentów potwierdzających utylizację materiałów w ilościach odpowiadających faktycznemu zakresowi wykonanych prac.

3.2 Budowa tras kablowych

Wszystkie trasy kablowe muszą być wykonane zgodnych z dyrektywą 2006/95/WE, w sposób pozwalający na zachowanie odpowiednich promieni gięcia wiązek kablowych na zakrętach. Wartości minimalnych promieni gięcia kabli są podane w kartach katalogowych kabli miedzianych i światłowodowych. Przy budowie tras kablowych pod potrzeby okablowania strukturalnego należy wziąć pod uwagę zapisy normy EN 50174-2:2009 lub równoważnej, dotyczące równoległego prowadzenia różnych instalacji w budynku, m.in. instalacji zasilającej, zachowując odpowiednie odległości pomiędzy okablowaniem zasilającym, a okablowaniem strukturalnym przy jednoczesnym uwzględnieniu materiału, z którego zbudowane są kanały kablowe. W ciągach komunikacyjnych kable prowadzić w korytach metalowych podsufitowo, w pokojach natynkowo w korytach kablowych z tworzyw sztucznych. W pomieszczeniu technicznym sąsiadującym z serwerownią, główne ciągi wykonać podsufitowo w korytach metalowych, pionowe zejścia w peszlach podtynkowo. W miarę możliwości należy wykorzystać istniejące trasy kablowe, w tym szachty kablowe. Po zakończeniu prac instalacyjnych wymagane jest odtworzenie zabezpieczenia przejść instalacyjnych. W zakresie instalacji teletechnicznych i elektrycznych nie dopuszcza się przeciągania przewodów przez przepusty ścianowe i między stropowe bez wprowadzania w nie dodatkowych zabezpieczeń uniemożliwiające uszkodzenia kabli w trakcie przeciągania. Jako osłony przed przypadkowymi uszkodzeniami mechanicznymi należy stosować rury stalowe, rury z tworzyw sztucznych, korytka blaszane itp. Rozmiary (pojemność) kanałów kablowych (dotyczy również peszli instalowanych w pomieszczeniu technicznym) należy dobierać w zależności od maksymalnej liczby kabli projektowanych w danym miejscu instalacji. Należy przyjąć zapas 20% na potrzeby ewentualnej rozbudowy systemu. Zajętość światła kanałów kablowych przez kable należy obliczać w miejscach zakrętów kanałów kablowych. Przy całkowitym wypełnieniu światła kanału kablami na zakręcie kanał będzie wówczas wypełniony w 40% na prostym odcinku. W peszlach pozostawić piloty dla potrzeb ewentualnego wprowadzenia dodatkowych kabli na etapie eksploatacji. Nie dopuszcza się montażu tras kablowych na żadnym z odcinków na kleju natynkowym, a jedynie z wykorzystaniem kołków montażowych. Wykonawca wykonując trasy kablowe dla sieci teleinformatycznej jest zobowiązany do szczególnej ostrożności w czasie realizacji bruzdowania, wykonania otworów w ścianach oraz odwiertów i przekuć przez ściany lub

stropy w zakresie istniejących wiązek kabli elektrycznych, rur i innych elementów budynku ukrytych pod tynkiem które muszą pozostać nieuszkodzone.

3.3 Układanie Kabli

Przy układaniu kabli, zarówno miedzianych, jak i światłowodowych należy stosować się do odpowiednich zaleceń producenta (tj. promienia gięcia, siły i sposobu wciągania, itp.).

Symetryczne kable skrętkowe należy układać w wybudowanych kanałach kablowych w sposób odpowiadający odporności konstrukcji kabla na wszelkie uszkodzenia mechaniczne. W szczególności należy wystrzegać się nadmiernego ściskania kabli, deptania po kablach ułożonych na podłodze oraz załamywania kabli na elementach konstrukcji kanałów kablowych. Przy odwijaniu kabla z bębna bądź wyciąganiu kabla z pudełka nie należy przekraczać maksymalnej siły ciągnięcia oraz zwracać uwagę na to, by na kablu nie tworzyły się węzły ani supły. Przyjęty ogólnie promień gięcia podczas instalacji wynosi 8-krotność średnicy zewnętrznej kabla skrętkowego.

3.4 Budowa gniazd użytkowników

Punkty dostępu do systemu są zrealizowane w formie gniazd montowanych na listwach natynkowych. Doprowadzenie kabli do gniazd wiąże się z pozostawieniem zapasu kabla w obrębie gniazda bądź tuż za nim w sytuacjach, kiedy gabaryty gniazda nie pozwalają na zorganizowanie zapasu. Instalacja gniazd musi uwzględniać łatwy dostęp użytkowników do gniazd. Gniazdo ma być zgodne ze standardem uchwytu osprzętu elektroinstalacyjnego typu Mosaic (45x45mm) i zawierać zacisk zapewniający optymalne mocowanie kabla.

3.5 Trasowanie

Trasa instalacji okablowania strukturalnego powinna przebiegać bezkolizyjnie z innymi instalacjami i urządzeniami, powinna być przejrzysta, prosta i dostępna dla prawidłowej konserwacji oraz remontów. W przypadku długich traktów, gdzie kable sieci teleinformatycznej i zasilającej biegną równolegle do siebie na odległości większej niż 35m, należy zachować odległość między instalacjami, co najmniej 10mm lub stosować metalowe przegrody. Kable stosowane w różnych celach (np. zasilające energią elektryczną i informatyczne) nie powinny być umieszczane w tych samych wiązkach. Różne wiązki powinny być oddzielone elektromagnetycznie od siebie. Szczegółowe informacje w normie EN 50174-1:2009 lub równoważnej.

3.6 Przejścia przez ściany i stropy

Przejścia przez ściany i stropy powinny spełniać następujące wymagania:

- wszystkie przejścia obwodów instalacji okablowania strukturalnego przez ściany
- i stropy itp. muszą być chronione przed uszkodzeniami,

- przejścia te należy wykonywać w przepustach rurowych
- obwody instalacji okablowania strukturalnego przechodząc przez podłogi muszą
- być chronione do wysokości bezpiecznej przed przypadkowymi uszkodzeniami.

Jako osłony przed przypadkowymi uszkodzeniami mechanicznymi należy stosować rury stalowe, rury z tworzyw sztucznych, korytka blaszane itp.

4. Materiały

Parametry techniczne materiałów i wyrobów powinny być zgodne z wymaganiami podanymi w projekcie i powinny odpowiadać wymaganiom obowiązujących norm państwowych (PN) oraz przepisom dotyczącym instalacji okablowania strukturalnego i instalacji urządzeń systemów bezpieczeństwa instalowanych obiektach.

Zamawiający dopuści do użycia tylko te materiały, które posiadają:

- certyfikat na znak bezpieczeństwa wykazujący, że zapewniono zgodność z kryteriami technicznymi określonymi na podstawie Polskich Norm, aprobat technicznych oraz właściwych przepisów i dokumentów technicznych,
- deklarację zgodności lub certyfikat zgodności z: Polską Normą, aprobatą techniczną, w przypadku wyrobów, dla których nie ustanowiono Polskiej Normy, jeżeli nie są objęte certyfikacją określoną w pakt 1 i które spełniają wymogi Szczegółowego Opisu Przedmiotu Zamówienia.

W przypadku materiałów, dla których ww. dokumenty są wymagane, każda partia dostarczona do realizacji robót musi posiadać te dokumenty, określające w sposób jednoznaczny cechy produktu. Produkty przemysłowe muszą posiadać w/w dokumenty wydane przez producenta.

Jakiekolwiek materiały, które nie spełniają tych wymagań jakościowych będą odrzucone.

Wszystkie dostarczone elementy systemu okablowania LAN oraz urządzenia sieciowe muszą być oznakowane znakiem CE zgodnie z wymogami deklaracji zgodności UE wystawionej przez producenta lub jego upoważnionego przedstawiciela, w celu potwierdzenia zgodności z dyrektywami Nowego Podejścia lub równoważnym.

5. Odbiór

Sieć LAN oraz dedykowane elektryczne zasilanie dla celów teleinformatycznych będzie podlegało odbiorowi przez Zamawiającego poprzez przeprowadzenie testów wykonanych sieci na obiekcie oraz na wybranych usługach, które powinny być możliwe do zrealizowania w zakresie zbudowanej sieci teleinformatycznej. Odbiór wykonanych robót będzie obejmował:

- weryfikację struktury systemu okablowania;
- weryfikacja wydajności systemu okablowania;

- weryfikacja jakości wykonania prac wykończeniowych;
- weryfikację sprawności działania dostarczonych urządzeń i systemów;
- weryfikację dokumentacji powykonawczej.

6. Przepisy prawne i normy związane z projektowaniem i wykonaniem przedmiotu zamówienia

Ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. 2019 r. poz. 2019 ze zm.).

Ustawa z dnia 7.07.1994 Prawo budowlane (Dz.U. 2020 r. poz. 1333 ze zm.) oraz przepisami wykonawczymi do tej ustawy.

Rozporządzenia Ministra Infrastruktury z 18.05.2004. w sprawie określenia metod i podstaw sporządzania kosztorysu inwestorskiego. (Dz.U. 2004 r. Nr 130 poz. 1389).

Rozporządzenie Ministra Infrastruktury z dnia 02.09. 2004 r. w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych (Dz.U. z 2013 r.poz.1129).

Rozporządzenie Ministra Infrastruktury z dnia 6 lutego 2003 r. w sprawie bezpieczeństwa i higieny pracy podczas wykonywania robót budowlanych (Dz.U. Nr 47, poz. 401).

Norma branżowa PN-IEC 60364 – Instalacje elektryczne w obiektach budowlanych.

Norma branżowa PN-EN 50173-1 Technika informatyczna – Systemy okablowania strukturalnego. Cz1. Wymagania ogólne i strefy biurowe.

Norma branżowa PN-EN 50174-1 Technika informatyczna – Instalacja okablowania. Cz1. Instalacja okablowania.

Norma branżowa PN-EN 50174-2 Technika informatyczna – Instalacja okablowania. Cz2. Planowanie i wykonawstwo instalacji wewnątrz budynków.

Norma branżowa PN-EN 50346 – Technika informatyczna – Instalacja okablowania. Badanie zainstalowanego okablowania.

Norma branżowa PN-EN 61935-1:2010 - Wymagania dotyczące sprawdzania symetrycznych i współosiowych kablowych linii telekomunikacyjnych - Część 1: Okablowanie z symetrycznych kabli telekomunikacyjnych zgodne z serią norm EN 50173.

Norma branżowa PN-EN50310:2012 Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanym sprzętem informatycznym.

ISO/IEC 11801-1:2017 - Information technology - Generic cabling for customer premises - Part 1: General requirements.

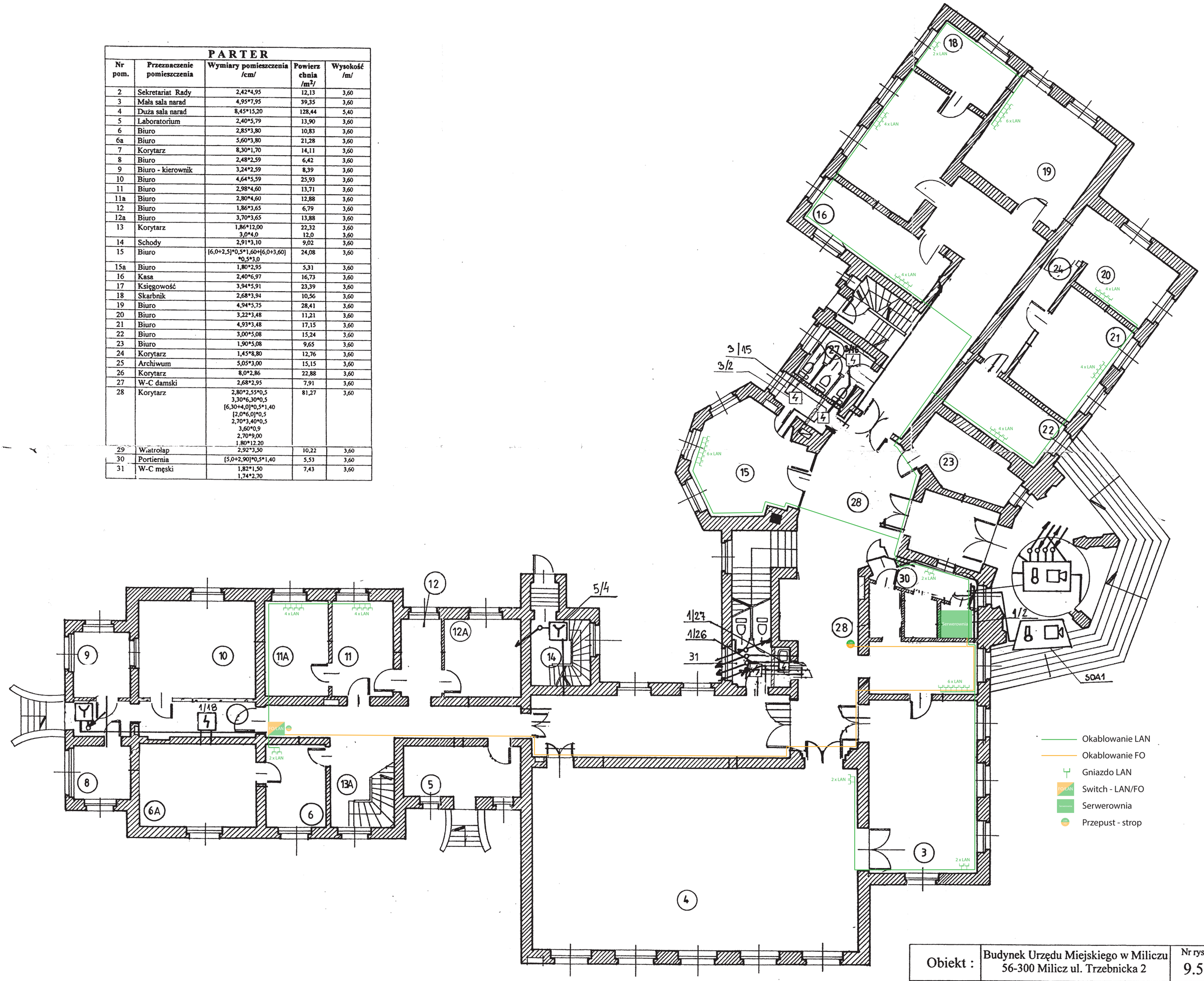
ISO/IEC 11801-2:2017 - Information technology - Generic cabling for customer premises - Part 2: Office premises.

ISO/IEC TR 24750:2007 - Information technology - Assessment and mitigation of installed balanced cabling channels in order to support 10GBASE-T

7. Minimalne Zestawienie Materiałowe

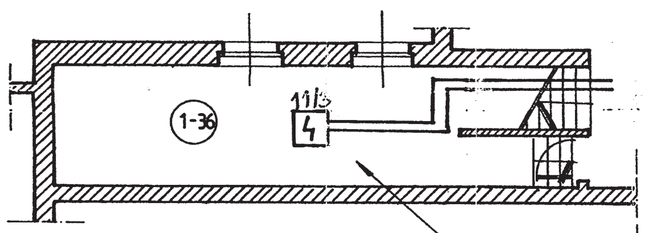
l.p.	Instalacja sieci komputerowej_LAN	jednostka	ilość	branża
1	Szafa Rack 12 U 800x1000	szt	1	LAN
1	Szafa Rack 6U x600 mm wisząca	szt.	3	LAN
2	Kabel F/UTP cat.6 A	mb	10 000	LAN
3	Patchpanel kat 6 FTP 24xRJ45	szt.	12	LAN
4	Moduł F/UTP kat. 6A podwojne	szt.	94	LAN
5	Gniazdo RJ45 typ 45/45 kat. 6A podwójne	szt.	94	LAN
6	Patchkordy kat. 6F/UTP 1m	szt.	200	LAN
7	Patchkordy kat. 6F/UTP 7m	szt.	10	LAN
8	Koryto PCV do montażu osprzętu Mosaic 45x45	mb.	2000	LAN
9	Światłowód jednomodowy 12 włóknowy złącze LC-LC	mb.	600	LAN
10	Przełącznik sieciowy	szt.	5	LAN

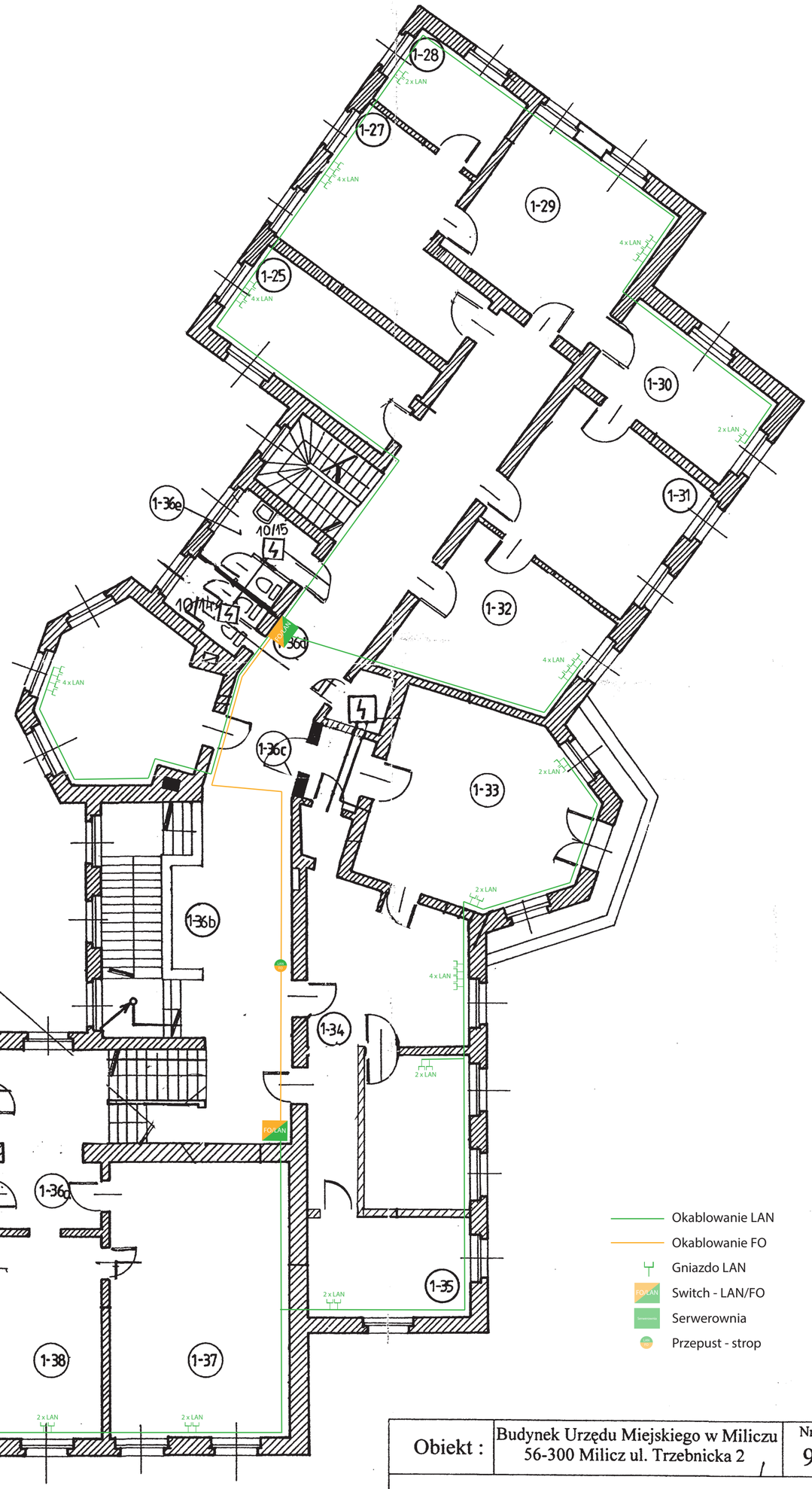
PARTER				
Nr pom.	**Przeznaczenie pomieszczenia**	**Wymiary pomieszczenia /cm/**	**Powierzchnia /m²/**	**Wysokość /m/**
2	Sekretariat Rady	2,42*4,95	12,13	3,60
3	Mała sala narad	4,95*7,95	39,35	3,60
4	Duża sala narad	8,45*15,20	128,44	5,40
5	Laboratorium	2,40*5,79	13,90	3,60
6	Biuro	2,85*3,80	10,83	3,60
6a	Biuro	5,60*3,80	21,28	3,60
7	Korytarz	8,30*1,70	14,11	3,60
8	Biuro	2,48*2,59	6,42	3,60
9	Biuro - kierownik	3,24*2,59	8,39	3,60
10	Biuro	4,64*5,59	25,93	3,60
11	Biuro	2,98*4,60	13,71	3,60
11a	Biuro	2,80*4,60	12,88	3,60
12	Biuro	1,86*3,65	6,79	3,60
12a	Biuro	3,70*3,65	13,88	3,60
13	Korytarz	1,86*12,00 3,0*4,0	22,32 12,0	3,60 3,60
14	Schody	2,91*3,10	9,02	3,60
15	Biuro	[6,0+2,5]*0,5*1,60+[6,0+3,60]*0,5*3,0	24,08	3,60
15a	Biuro	1,80*2,95	5,31	3,60
16	Kasa	2,40*6,97	16,73	3,60
17	Księgowość	3,94*5,91	23,39	3,60
18	Skarbnik	2,68*3,94	10,56	3,60
19	Biuro	4,94*5,75	28,41	3,60
20	Biuro	3,22*3,48	11,21	3,60
21	Biuro	4,93*3,48	17,15	3,60
22	Biuro	3,00*5,08	15,24	3,60
23	Biuro	1,90*5,08	9,65	3,60
24	Korytarz	1,45*8,80	12,76	3,60
25	Archiwum	5,05*3,00	15,15	3,60
26	Korytarz	8,0*2,86	22,88	3,60
27	W-C damski	2,68*2,95	7,91	3,60
28	Korytarz	2,80*2,55*0,5 3,30*6,30*0,5 [6,30+4,0]*0,5*1,40 [2,0*6,0]*0,5 2,70*3,40*0,5 3,60*0,9 2,70*9,00 1,80*12,20	81,27	3,60
29	Wiatrołap	2,92*3,50	10,22	3,60
30	Portiernia	[5,0+2,90]*0,5*1,40	5,53	3,60
31	W-C męski	1,82*1,50 1,74*2,70	7,43	3,60

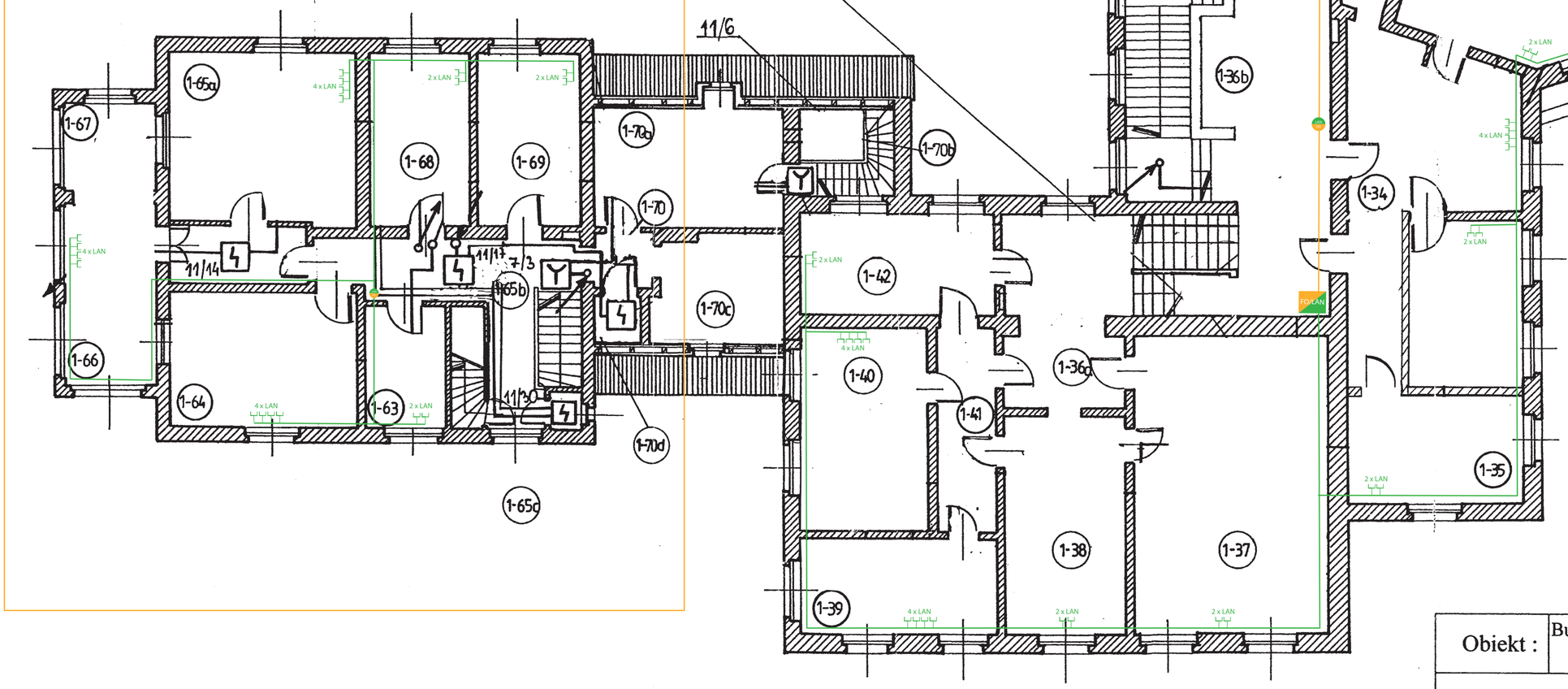


Obiekt :	Budynek Urzędu Miejskiego w Miliczu 56-300 Milicz ul. Trzebnicka 2	Nr rys. 9.5
Rzut parteru		SKALA 1:100

PIERWSZE PIĘTRO				
Nr pom.	Przeznaczenie pomieszczenia	Wymiary pomieszczenia /cm/	Powierzchnia /m²/	Wysokość /m/
1-24	Biuro	[2,50+6,0]*0,50*1,70+[3,2+6,0]*0,5*3,50	23,33	3,25
1-25	Biuro	7,05*3,21	22,63	3,25
1-26	Biuro	2,39*7,05	16,85	3,25
1-27	Biuro	4,0*2,55	10,20	3,25
1-28	Biuro	4,0*2,53	10,12	3,25
1-29	Biuro	5,76*5,20	29,95	3,25
1-30	Biuro	5,15*3,37	17,36	3,25
1-31	Biuro	4,80*5,15	24,72	3,25
1-32	Biuro	[5,5+3,79]*0,5*5,15	23,92	3,25
1-33	Burmistrz	4,57*6,0+[6 ,0+2,801]*0,5*2,50	38,42	3,25
1-34	Sekretariat	[5,50+3,94]*0,5*5,20+2,50*1,5	20,79	3,25
1-35	Burmistrz	5,20*8,11	42,17	3,25
1-36	Archiwum	2,90*12,0	34,80	2,20
1-36a	Korytarz	3,58*5,50	19,69	3,30
1-36b	Korytarz	2,70*[*12,0+15,70]	74,79	3,30
1-36c	Pom. gospodarcze	1,50*1,50	2,25	3,30
1-36d	Pom. gospodarcze	1,50*1,50	2,25	3,30
1-36e	W-C	4,75*2,95	14,01	3,30
1-37	Sala ślubów	5,65*8,50	48,03	3,30
1-38	Sala toastów	3,50*6,50	22,75	3,30
1-39	Kierownik U.S.C.	6,50*3,71+1,80*2,70	28,97	3,30
1-40	Biuro	2,30*3,70	8,51	3,30
1-41	Korytarz	1,65*5,80	9,57	3,30
1-42	Sekretarz Urzędu	2,98*4,72	14,06	3,30
1-63	Biuro	2,22*4,0	8,88	3,25
1-64	Biuro	5,45*4,0	21,8	3,25
1-65	Korytarz	4,0*1,50	6,0	3,25
1-65a	Pomieszczenie biurowe	5,48*4,96	27,18	3,25
1-65b	Korytarz	2,60*3,60+1,70*7,50	22,11	3,25
1-65c	W-C	0,90*1,0	0,90	3,25
1-66	Biuro	5,13*2,65	13,59	3,25
1-67	Biuro	2,64*2,2	6,65	3,25
1-68	Biuro	2,81*4,96	13,94	3,25
1-69	Biuro	3,05*4,96	15,13	3,25
1-70	Korytarz	1,60*1,50	2,40	3,25
1-70a	Powielarnia	5,50*4,0	22,0	3,25
1-70b	Klatka schodowa	2,60*2,60	6,76	3,25
1-70c	Powielarnia	4,0*3,0	12,0	3,25
1-70d	Pom. gospodarcze	1,30*1,50	1,95	3,25





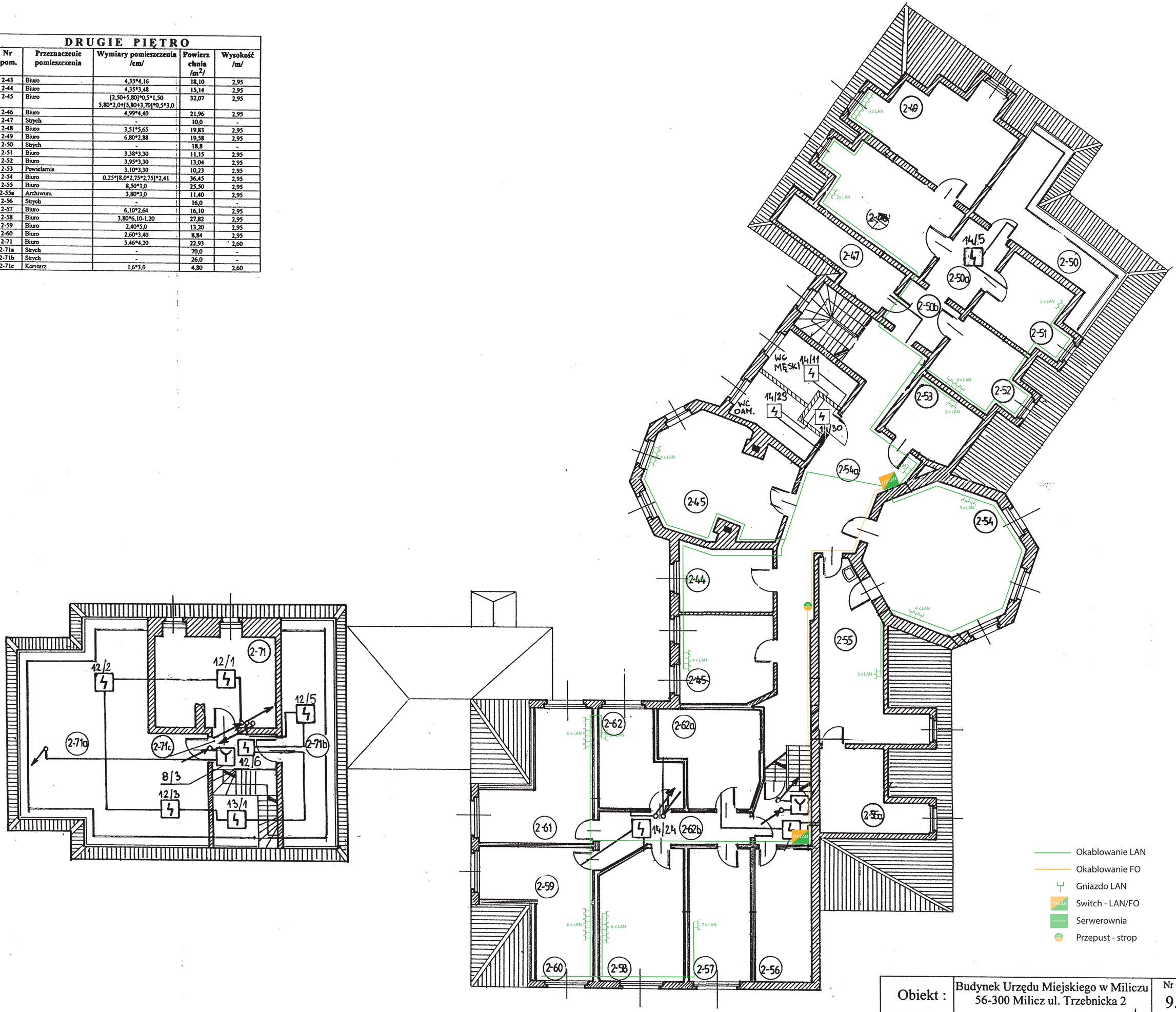


- Okablowanie LAN
- Okablowanie FO
- Gniazdo LAN
- Switch - LAN/FO
- Serwerownia
- Przepust - strop

Obiekt :	Budynek Urzędu Miejskiego w Miliczu 56-300 Milicz ul. Trzebnicka 2	Nr rys. 9.6
Rzut I piętra		

DRUGIE PIĘTRO

Nr pom.	Przeznaczenie pomieszczenia	Wymiary pomieszczenia /cm/	Powierzchnia /m^2/	Wysokość /m/
2-43	Biuro	4,35*4,16	18,10	2,95
2-44	Biuro	4,35*3,48	15,14	2,95
2-45	Biuro	[2,50+5,80]*0,5*1,50 5,80*2,0+[5,80+3,70]*0,5*3,0	32,07	2,95
2-46	Biuro	4,99*4,40	21,96	2,95
2-47	Strych	-	10,0	-
2-48	Biuro	3,51*5,65	19,83	2,95
2-49	Biuro	6,80*2,88	19,58	2,95
2-50	Strych	-	18,8	-
2-51	Biuro	3,38*3,30	11,15	2,95
2-52	Biuro	3,95*3,30	13,04	2,95
2-53	Powielarnia	3,10*3,30	10,23	2,95
2-54	Biuro	0,25*[8,0*2,75*2,75]*2,41	36,45	2,95
2-55	Biuro	8,50*3,0	25,50	2,95
2-55a	Archiwum	3,80*3,0	11,40	2,95
2-56	Strych	-	16,0	-
2-57	Biuro	6,10*2,64	16,10	2,95
2-58	Biuro	3,80*6,10-1,20	27,82	2,95
2-59	Biuro	2,40*5,0	13,20	2,95
2-60	Biuro	2,60*3,40	8,84	2,95
2-71	Biuro	5,46*4,20	22,93	2,60
2-71a	Strych	-	70,0	-
2-71b	Strych	-	26,0	-
2-71c	Korytarz	1,6*3,0	4,80	2,60



Obiekt :	Budynek Urzędu Miejskiego w Miliczu 56-300 Milicz ul. Trzebnicka 2	Nr rys. 9.7
Rzut II piętra		SKALA 1:100