Załącznik nr 1 do SWZ

Program Funkcjonalno-Użytkowy dla zadania pn.:
Cyfryzacja Urzędu Gminy i Miasta Łapy – doposażenie serwerowni oraz modernizacja sieci strukturalnej LAN w budynku Urzędu Miejskiego w Łapach.

Nazwa zamówienia:	**Cyfryzacja Urzędu Miejskiego w Łapach – doposażenie serwerowni oraz modernizacja sieci LAN**
Lokalizacja:	**Budynek UM Łapy ul. Sikorskiego 24, działki o nr: 1829/1; 993/1;**
Zamawiający:	**Gmina Łapy** **ul. Wł. Sikorskiego 24, 18-100 Łapy**
Nazwa i kody:	**Lista nazw i kodów ze Wspólnego Słownika Zamówień umieszczono na str. 2**
Data opracowania:	**czerwiec 2022r**
Autor:	**Robert Bogdanowicz**

Nazwa i kod wg. Wspólnego Słownika Zamówień:

Kod: 316 82530-4	Awaryjne urządzenia energetyczne
Kod: 450 00000-7	Roboty budowlane
Kod: 453 00000-0	Roboty w zakresie instalacji budowlanych
Kod: 453 10000-3	Roboty instalacyjne elektryczne
Kod: 453 11000-0	Roboty w zakresie okablowania strukturalnego oraz instalacji elektrycznych
Kod: 453 11100-1	Roboty w zakresie okablowania elektrycznego
Kod: 453 11200-2	Roboty w zakresie instalacji elektrycznych
Kod: 453012000-7	Instalowanie systemów alarmowych i anten
Kod: 453 12100-8	Instalowanie przeciwpożarowych systemów alarmowych
Kod: 453 12200-9	Instalowanie przeciwwłamaniowych systemów alarmowych
Kod: 453 14300-4	Instalowanie infrastruktury okablowania
Kod: 453 14310-7	Układanie kabli
Kod: 453 14320-0	Instalowanie okablowania komputerowego
Kod: 453 15600-4	Instalacje niskiego napięcia
Kod: 453 31200-8	Instalowanie urządzeń wentylacyjnych i klimatyzacyjnych
Kod: 454 21131-1	Instalowanie drzwi
Kod: 454 32121-8	Roboty w zakresie podłóg w pomieszczeniach komputerowych
Kod: 454 53000-7	Roboty remontowe i renowacyjne
Kod: 710 00000-8	Usługi architektoniczne, budowlane, inżynieryjne i kontrolne
Kod: 710 24000-2	Usługi architektoniczne, inżynieryjne i planowania
Kod: 712 00000-0	Usługi architektoniczne i podobne
Kod: 713 00000-1	Usługi inżynieryjne
Kod: 713 20000-7	Usługi inżynieryjne w zakresie projektowania
Kod: 715 00000-3	Usługi związane z budownictwem

Spis treści

1. Część opisowa

1.1 *Opis ogólny przedmiotu zamówienia*

Program funkcjonalno–użytkowy opisuje ilościowo i jakościowo elementy, które będą przedmiotem zamówienia w drodze postępowania przetargowego.

Przyszły Wykonawca zobowiązany będzie zrealizować zamówienie w dwóch etapach:

- opracowanie dokumentacji projektowej,
- dostawa urządzeń i materiałów oraz wykonanie robót.
- wdrożenie urządzeń i szkolenia.

Przedmiotem zadania jest zaprojektowanie i wykonanie dostaw i prac składających się na zadanie „Cyfryzacja Urzędu Gminy i Miasta Łapy – doposażenie serwerowni oraz modernizacja sieci LAN”

Ramowy zakres dostaw i prac obejmuje następujący zakres:

- projekt wykonawczy na potrzeby doposażenia serwerowni oraz modernizacji sieci LAN,
- wykonanie okablowania i gniazd LAN w budynku,
- wykonanie punktów pośrednich i łączników światłowodowych,
- dostawa i konfiguracja urządzeń aktywnych na potrzeby sieci LAN,
- dostawa i wdrożenie serwerów z oprogramowaniem i licencjami,
- wdrożenie systemu zabezpieczenia cyfrowego klasy UTM,
- modernizacja układu zasilania elektrycznego serwerowni wraz z elementami zabezpieczeń,
- dostawa i wdrożenie systemów monitorowania i zabezpieczeń technicznych serwerowni,
- wykonanie dokumentacji pomiarowej i dokumentacji powykonawczej.
- przeszkolenie administratorów

Wszelkie urządzenia dostawy i roboty nie ujęte szczegółowo w niniejszym opracowaniu a niezbędne do prawidłowego wykonania i funkcjonowania pisanych powyżej zakresów winne być zaprojektowane i wykonane przez Wykonawcę. Efektem końcowym przeprowadzonych prac i dostaw powinno być kompletne zadanie spełniające funkcjonalności i wymagania opisane w poniższym dokumencie.

W przypadku, gdy w niniejszym opisie przedmiotu zamówienia lub jego załącznikach podano nazwy własne materiałów, produktów lub urządzeń wskazujące na konkretnych producentów to należy traktować to jedynie jako określenie pożądanego standardu i jakości. We wszystkich takich sytuacjach Wykonawca może zaoferować równoważne materiały, produkty lub urządzenia o co najmniej takich samych parametrach. Przez równoważność produktu rozumie się zaoferowanie

produktu, którego parametry techniczne zastosowanych materiałów są co najmniej takie same jak produktów opisanych w tym dokumencie. W przypadku zaoferowania rozwiązania równoważnego, Wykonawca zobowiązany jest wykazać równoważność lub wyższość zastosowanych rozwiązań.

1.1.1 Charakterystyczne parametry określające zakres dostaw i robót budowlanych

Parametry ilościowe określające zakres robót budowlanych wynika z przyjętej przez Zamawiającego koncepcji wstępnej dla tego zadania. W zakresie zadania wydzielić możemy poniższe parametry określające zakres dostaw i usług.

- adaptacja, modernizacja i doposażenie pomieszczeń serwerowni: 1
- ilość węzłów sieciowych pośrednich: 1
- szacowana łączna ilość podwójnych punktów logicznych: 70
- dostawa serwera sprzętowego: 2
- dostawa urządzenia klasy UTM: 1
- system zasilania rezerwowego: 2

1.1.2 Aktualne uwarunkowania wykonania przedmiotu zamówienia

W przedmiotowym obiekcie wydzielono pomieszczenie spełniające obecnie funkcjonalność serwerowni. W pomieszczeniu znajduje się szafa teletechniczna 19” oraz inne urządzenia techniczne. W budynku urzędu zlokalizowana jest również sieć logiczna która obsługuje jednostkę i procesy niezbędne do funkcjonowania Urzędu Miejskiego. Okablowanie logiczne budynku wykonane jest kablami miedzianymi FUTP kat 5. Kable prowadzone są zarówno w korytach kablowych jak i w przestrzeniach podsufitowych. W obrębie sieci LAN wyróżnić możemy dwa węzły, jednym z nich jest serwerownia znajdująca się na parterze w pomieszczeniu serwerowni rys.1 oraz naścienna szafka dystrybucyjna znajdująca się na 2 piętrze w pomieszczeniu obok pokoju nr 203 rys.2.

Główna serwerownia urzędu znajduje się w pomieszczeniu zlokalizowanym na parterze budynku. Pomieszczenie ma wymiary 2,90m x 1,65m i wysokość 3,15 m. Stan pomieszczenia ogólny jest dobry, ściany i sufit są tynkowane i malowane, wykończenie podłogi stanowi gres szkliwiony. Pomieszczenie nie posiada okien a jedynie drzwi wychodzące na korytarz.

Przedsięwzięcie realizowane jest w formule zaprojektuj i wybuduj, tym samym w celu oszacowania i wyceny zakresu robót przedmiotu zamówienia należy:

- przeprowadzić wizje lokalną w budynku i dokonać własnej inwentaryzacji,
- zapoznać się z stanem istniejącym,
- przestrzegać zapisów i wymagań niniejszego PFU,
- przeprowadzić własne szacowanie i obmiary ilościowe.

Przy szacowaniu kosztów Wykonawca powinien liczyć się z faktem, iż rodzaj i ilość robót opisany w programie funkcjonalno-użytkowym może ulec zmianie w trakcie wykonania dokumentacji projektowej. Szczegółowe rozwiązania wpływające na zwiększenie zakresu i ilości robót stanowią ryzyko Wykonawcy i nie są traktowane jako roboty dodatkowe.

Zamawiający wymaga przedłożenia przez Wykonawcę rozwiązań projektowych celem ich oceny i akceptacji.

1.1.3 Ogólne właściwości funkcjonalno-użytkowe

Instalacje i urządzenia dostarczone i wbudowane w ramach przedmiotowego zadania powinny spełniać opisane poniżej parametry techniczne oraz być kompatybilne z aktualnie funkcjonującymi systemami Zamawiającego.
Nowobudowane węzły i punkty logiczne LAN należy wyposażyć w urządzenia aktywne umożliwiające obsługę wskazanej ilości punktów logicznych zapewniając jednocześnie rezerwę na poziomie 30 % portów aktywnych. Okablowanie strukturalne i wszystkie elementy toru powinny spełniać minimum klasę EA. Wewnętrzna sieć lokalną urzędu należy zabezpieczyć rozwiązaniem sprzętowym klasy UTM o podanych poniżej parametrach minimalnych.
Główne funkcjonalności ogólne systemu:

- pełna obsługa w zakresie połączeń LAN wszystkich stanowisk urzędu i urządzeń sieciowych,
- przeprowadzenie analizy zagrożeń i zapewnienie ochrony cyfrowej wewnętrznej sieci informatycznej z wykorzystaniem dostarczonej zapory,
- zapewnienie podstawowej ochrony technicznej pomieszczenia serwerowni,

- zapewnienie stabilnego gwarantowanego systemu zasilania energetycznego serwerowni,
- wdrożenie systemu monitorowania parametrów środowiskowych w serwerowni.

1.2 Opis wymagań Zamawiającego w stosunku do przedmiotu zamówienia

1.2.1 Dokumentacja wykonawcza

Wykonawca zobowiązany jest do wykonania wszystkich dokumentacji i projektów wymaganych do zrealizowania zadania. Dokumentacja musi być opracowana zgodnie z obowiązującymi przepisami i zasadami wiedzy technicznej. W szczególności musi uwzględniać przepisy:

- Ustawa z dnia 7 lipca 1994 r. - Prawo budowlane (Dz.U. 1994 Nr 89 poz. 414) z późniejszymi zmianami,
- Rozporządzenie Ministra Infrastruktury z dnia 2 września 2004 r. w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych,
- Prawo Ochrony Środowiska Ustawa z dnia 27 kwietnia 2001r Dz. U. Nr 62/2001r z późniejszymi zmianami,

Dokumentacja wykonawcza zostanie przedstawiona Zamawiającemu do akceptacji i zatwierdzenia przed przystąpieniem do wykonania prac. Dokumentacja powinna zawierać wszystkie dane techniczne, lokalizacyjne i zestawienia materiałowe. Projekt wykonawczy powinien umożliwiać kompleksowe wykonanie przedmiotu zamówienia bez konieczności sporządzania dodatkowych opracowań i uzgodnień.
Dokumentacja wykonawcza w szczególności powinna zawierać:

- branżowe projekty wykonawcze,
- opis przyjętych rozwiązań technicznych,
- plan sytuacyjny rozmieszczenia punktów logicznych i dystrybucyjnych,
- plan tras kablowych,
- zestawienie materiałów i urządzeń,
- plan topologii, zestawienia, numeracja i adresacja sieci LAN,
- specyfikacji technicznych wykonania i odbioru robót,
- obliczenia i obmiary,

- planu BIOZ (przy robotach, które tego wymagają).

Dokumentację projektową w powyższym zakresie należy opracować dla serwerowni i sieci strukturalnej budynku, zasilania i pozostałych systemów. Projekty technologiczny serwerowni powinny przedstawiać sposób umieszczenia urządzeń w serwerowniach tj. szaf serwerowych, rozdzielni elektrycznych, UPS, klimatyzatorów, pozostałych instalacji teletechnicznych. W dokumencie tym należy przedstawić wzajemne usytuowanie wszystkich urządzeń wbudowanych i zinwentaryzowanych w pomieszczeniu serwerowni. Cała kompletna dokumentacja projektowa powinna być wykonana w wersji papierowej oraz elektronicznej w postaci plików edytowalnych. Wykonana dokumentacja projektowa musi zawierać wszelkie zgody, uzgodnienia, opinie i decyzje wymagane do prawidłowej realizacji wszystkich prac budowlanych i montażowych. Po zakończeniu robót wykonawca musi dostarczyć dokumentację powykonawczą wykonanych prac wraz z pomiarami w 2 egzemplarzach.

1.2.2 Prace budowlane w serwerowni

Pomieszczenie serwerowni należy zmodernizować i doposażyć we wskazane w dalszej części opracowania urządzenia. Urządzenia należy zainstalować w istniejącej szafie teleinformatycznej po uprzedniej inwentaryzacji oraz uporządkowaniu przestrzeni instalacyjnej i okablowania.
W serwerowni należy wykonać prace około budowlane w następujących zakresach:

- opracować projekt wykonawczy modernizacji serwerowni,
- wykonać koryta i trasy kablowe,
- wykonać przyłącze energetyczne wraz z dedykowaną rozdzielnią i instalacja elektryczną,
- wydzielić serwerownię jako odrębną strefę pożarową, wykonać niezbędne prace budowlane dostosowujące drzwi wejściowe i uszczelnienia,
- wykonać prace nieujęte powyżej, a będące koniecznymi przy pracach budowlanych takie jak, naprawa tynków, podłogi, malowanie ścian, inne.

Podłoga serwerowni powinna zachować parametry antyelektrostatyczności wykonana w postaci powłoki lub wykładziny o trudno-zapalnym stopniu palności. Drzwi do pomieszczenia powinny być wymienione na spełniające wymogi klasy C wg PN-90/B-92270 i PN-B/96-02871 dotyczące

odporności na włamanie i wymogi dotyczące wytrzymałości ogniowej min. EI 30 (30 minut) wg PN-EN-13501. Wykonać należy instalację uziemienia a w serwerowni należy zainstalować szynę ekwipotencjalna, do której podłączone będą wszystkie metalowe elementy urządzeń i szafa teletechniczna. Trasy kablowe przewodów elektrycznych, i sygnałowych oraz światłowodowych powinny być odseparowane od siebie. Wszelkie przebicia przez ściany i stropy powinny być uszczelnione przeciwpożarowo dla uzyskania właściwej odporności ogniowej.

1.2.3 Montaż drzwi klasy EI 30 w serwerowni

W zakresie prac jest demontaż starych i montaż nowych drzwi do pomieszczenia serwerowni. Nowe drzwi powinny spełniać poniższe wymagania.

- odporność na włamania standardowa do pomieszczenia serwerowni drzwi klasy C wg PN-90/B-92270 i PN-B/96-02871,
- norma wytrzymałości ogniowej min. EI 30 (30 minut) wg PN-EN-13501,
- aprobata normatywna - drzwi powinny posiadać wywieszkę – APROBATĘ NORMATYWNĄ wydaną przez ITB Instytut Techniki Budowlanej - przytwierdzoną z boku drzwi w wewnętrznej części framugi – skrzydła drzwi,
- drzwi przystosowane do montażu kontroli dostępu wyposażone w samozamykacz,
- drzwi wyposażone w dwa zamki (zamek kluczowy + kontrola bezpieczeństwa),
- próg w drzwiach - powinien być płaski, wyprofilowany bez progu.

Materiały użyte do uszczelnienia drzwi muszą spełniać wymagania i zalecenia norm przeciwpożarowych. Dotyczy to głównie pianek montażowych, które muszą posiadać odpowiednią klasę wytrzymałości PPOŻ. Cały proces wymiany powinien być udokumentowany w stosownym protokole, w którym będą potwierdzone informacje o klasie bezpieczeństwa drzwi i klasie bezpieczeństwa ich montażu.

1.2.4 Instalacje w serwerowni

W serwerowni należy wykonać instalacje z następującego zakresu:

- klimatyzację komfortu z pakietem do pracy całorocznej,
- okablowanie strukturalne światłowodowe i miedziane,

- przyłącze energetyczne wraz z rozdzielnią zasilania podstawowego serwerowni,
- systemy awaryjnego zasilania serwerowni,
- listwy zasilające zarządzane,
- system sygnalizacji włamania i napadu,
- system kontroli dostępu,
- system telewizji dozorowej,
- system monitoringu środowiskowego infrastruktury serwerowni (czujniki zalania, temperatury, wilgotności, czujnik dymu) ze zdalnym powiadomieniem za pomocą poczty elektronicznej i lub SMS.

1.2.5 Zasilanie podstawowe serwerowni

W ramach zapewnienia zasilania elektrycznego dla urządzeń w serwerownia należy:

- opracować projekt wykonawczy instalacji elektrycznej na potrzeby serwerowni,
- wykonać odpowiednie 3 fazowe przyłącze energetyczne z rozdzielni elektrycznej budynkowej NN,
- wykonać lokalną rozdzielnię elektryczną zasilania serwerowni,
- dostarczyć i uruchomić UPS-a w wersji RACK, z pełnym wyposażeniem (by-pass, instalacja, karta sieciowa, system nadzoru i monitoringu),
- wykonać obwody odbiorcze do szafy serwerowej na potrzeby instalacji listew zasilających zarządzanych,
- wykonać uziemienie i instalację połączeń wyrównawczych,
- wyposażyć obwody w niezbędne zabezpieczenia nadprądowe, różnicowoprądowe i przeciwprzepięciowe przewidziane dla tego typu obiektów,
- przebudować instalację oświetleniową i gniazd ogólnych w pomieszczeniu dostosowując do wymogów zawartych w normach,

System zasilania podstawowego w serwerowni spełnia poniższe warunki:

- zapotrzebowanie mocy urządzeń adekwatne do ilości zainstalowanych urządzeń (serwery, macierze, inne),

- tolerancja napięcia fazowego wynosi 230V ± 5%,
- zawartość harmonicznych w napięciu fazowym nie przekracza 5%,
- tolerancja częstotliwości wynosi 50Hz ± 5%,
- wartość skuteczna różnicy napięć pomiędzy przewodem N i PE w dowolnym gnieździe zasilającym nie przekracza 1V,

Zasilanie podstawowe serwerowni powinno uwzględniać moc urządzeń niezbędnych do prawidłowego funkcjonowania obiektu (w tym klimatyzacji i oświetlenia) oraz zapewniać rezerwę minimum 50% mocy na potrzeby doposażenia serwerowni w kolejne urządzenia.
Sposób wykonania zasilania w odniesieniu do warunków w budynku Urzędu Miejskiego określi projektant instalacji elektrycznych na etapie opracowywania dokumentacji projektowej.
Na potrzeby zasilenia serwerowni należy wykonać nowe połączenie kablowe z rozdzielni głównej budynku która znajduje się na tej samej kondygnacji budynku w korytarzu głównym. Od strony rozdzielni kabel należy doprowadzić do nowej rozdzielni, skąd zostaną wyprowadzone obwody serwerowni w tym obwodu gwarantowane (UPS), jak i obwody niegwarantowane (oświetlenie, gniazda na potrzeby ogólne w serwerowni).

1.2.6 Zasilanie rezerwowe

Na potrzeby rezerwowego podtrzymania pracy kluczowych urządzeń i systemów w serwerowni należy dostarczyć, zainstalować i uruchomić zasilacza awaryjny w wersji RACK z dodatkową baterią EBM. W przypadku zaniku napięcia w obwodzie podstawowym, obwody zasilania gwarantowanego zostają zasilone z bezprzerwowego zespołu UPS-a, zapewniając stabilne parametry sieci zasilającej wskazane urządzenia.
Moc UPS-a powinna być dobrana stosownie do przyjętego zapotrzebowania mocy kluczowych urządzeń w serwerowni. Moc urządzeń w serwerowni wstępnie szacuje się na ok 2500 W. Czas podtrzymania jest dobrany w zależności od czasu potrzebnego na kontrolowane wyłączenie urządzeń i szacowany jest na 30 minut. Zasilacz UPS powinien posiadać strukturę 3f/1f z możliwością konfiguracji trybu pracy 3f/1f oraz 1f/1f i moc minimum 7000 W i musi zapewnić czas podtrzymania minimum 5 minut dla obciążenia 5,0 kW, wraz za zasilaczem UPS musi zostać dostarczony dodatkowy moduł baterii EBM, który wydłuży czas podtrzymania do minimum 30 minut dla obciążenia 5,0 kW. Zasilacz UPS wykonany powinien być w architekturze podwójnej

konwersji on-line VFI. Zasilacz UPS wykonany w postaci uniwersalnej obudowy Tower/Rack. Urządzenie główne oraz moduły baterii muszą być dostarczone wraz z kompletem kabli i zestawem szyn do montażu w szafie rack. Cały system zasilania powinien zostać uruchomiony zgodnie z zaleceniami producenta.

Na potrzeby rezerwowego podtrzymania pracy kluczowych urządzeń i systemów w szafie punktu pośredniego należy dostarczyć, zainstalować i uruchomić zasilacza awaryjny w wersji RACK

Podstawowe parametry techniczno-eksploatacyjne UPS-a:

Parametry wejściowe

- napięcie: 380 V/400V/415V(3 fazowe),
- częstotliwość : 50 / 60 Hz + /-10% (ustawiana automatycznie, autodetekcja)
- współczynnik mocy/THDi : > 0,99 / < 5 %
- zakres napięcia by-pass: 40% ~ +15% (konfigurowalne)

Parametry wyjściowe:

- Napięcie (czysty przebieg sinusoidalny): 230 V (1-f) do wyboru 220 / 230 / 240VAC
- Częstotliwość : 50 /60 Hz + /- 1 % (+/- 0,1 Hz w trybie pracy bateryjnej)
- Zniekształcenia harmoniczne THDu ≤ 1% THD obciążenie liniowe | ≤ 3% THD obciążenie nieliniowe,
- Współczynnik mocy: 1
- Przeciążalność: min. 110 % przez 10 min ; 150 % przez 30 s

Bateria:

- Hermetyczne, bezobsługowe akumulatory o żywotności minimum 5 lat wg klasyfikacji EUROBAT umieszczone w obudowie bateryjnej.
- Czas ładowania < 8 godz. do odzyskania 90 % wydajności po całkowitym rozładowaniu
- Urządzenie musi posiadać alfanumeryczny wyświetlacz LCD wskazujący podstawowe parametry pracy,

Zasilacz UPS musi być wyposażony w, port RS232 (do obsługi protokołu MODBUS), RS485, wraz z zasilaczem UPS musi zostać dostarczona karta komunikacyjna SNMP i oprogramowanie do obsługi.

Zasilacz UPS musi być zgodny z Normami:

- Parametry i topologia: IEC 62040-3 (VFI-SS-111)
- Bezpieczeństwo: IEC/EN 62040-1,

- Kompatybilność elektromagnetyczna IEC/EN 62040-2
- Certyfikaty: CE,
- Stopień ochrony IP: min. IP20

Zasilacz UPS musi spełniać parametry środowiskowe co najmniej takie jak:

- Temperatura pracy od 0 °C do +40 °C,
- Wilgotność: 0% - 95 % bez kondensacji
- Poziom hałasu w odległości 1 m < 58 dB

Akcesoria dodatkowe muszą być wyprodukowane przez tego samego producenta co zasilacz UPS.

Urządzenie musi być objęte gwarancja producenta na okres co najmniej 36 miesięcy na moduł elektroniki oraz akumulatory.

1.2.7 Listwa zasilająca PDU zarządzalna

Dostawa, montaż i uruchomienie pionowej listwy zasilającej w istniejącej szafie 19”.

Podstawowe parametry listwy zasilającej z funkcją monitorowania:

- Min. 12 x Gniazdo komputerowe typu IEC320C13 16A/230V,
- Min. 4 x Gniazdo komputerowe typu IEC320C19 16A/230V,
- Gniazda podzielone na minimum dwa bloki. Każdy blok zabezpieczony wyłącznikiem nadmiarowo-prądowym MCB z charakterystyką C i ograniczeniem do 16A,
- Wyposażona ma być w gniazdo RJ45 do komunikacji Ethernet zgodnie z protokołem SNMP;
- Wyposażona w wskaźnik cyfrowy informujący o poborze prądu przez urządzenia aktywne,
- Wyposażona ma być w dodatkowe oprogramowanie umożliwiające zdalny monitoring poboru mocy na poszczególnych portach, aplikacja działająca w systemach Windows, lub dostępna poprzez przeglądarkę internetową,
- Listwa przystosowana do montażu w szafach 19" w pionie,
- Wsporniki do montażu listwy w 4 płaszczyznach,
- Kabel zasilający długości 3m,
- Maksymalne obciążenie 32A (7360 W),
- Stopień ochrony IP20,
- Deklaracja zgodności CE.

1.2.8 Doposażenie i okablowanie szafy w serwerowni i w miedzy piętrowym punkcie dystrybucji

Szafę w serwerowni oraz szafkę w punkcie pośrednim należy doposażyć w komponenty okablowania miedzianego i światłowodowego na potrzeby połączeń wewnętrznych serwerowni oraz połączeń międzywęzłowych i sieci strukturalnej całego budynku.
Szafa serwerowa i szafka w punkcie dystrybucji stanowi punkty podłączenia urządzeń końcowych (serwerów, macierzy dyskowych, przełączników, etc.). Szafy należy zmodernizować i doposażyć w zależności od potrzeb w:

- panele światłowodowe 19”/1U,
- panele krosowe 19” kategorii 6a,
- prowadnice kabli,
- kable krosowe światłowodowe,
- kable krosowe miedziane kat. 6a,
- półki i inne elementy instalacyjne.

Okablowanie pionowe (połączenie światłowodowe pomiędzy szafami)
Okablowanie pionowe (szkieletowe) łączy logicznie i fizycznie pośredni piętrowy punkt dystrybucyjny LAN z głównym punktem dystrybucyjnym znajdującym się w serwerowni za pomocą dwunastowłóknowego kabla światłowodowego jednomodowego (SM 9/125) lub wielomodowego (OM2 50/125). Łącznikowy kabel światłowodowy należy zakończyć w obydwu szafach na przełącznicach panelowych 19” złączami LC duplex. Kabel powinien być przeznaczony do układania wewnątrz budynków spełniając wymagania w zakresie materiałów nie wydzielających podczas pożaru szkodliwych gazów LSOH. Kabel wykonany zgodnie z normą: ISO/IEC 11801-1:2017; PN-EN 50173-1:2018.

Łącznik światłowodowy powinien spełniać poniższe wymagania:

- typ włókien, jednomodowe SM lub wielomodowe OM2, OM3 minimum 12 włókien,
- budowa w postaci luźnej tuby do układania wewnątrz, zmniejszony promień gięcia,

- średnia tłumienność jednostkowa: OM(1300nm)-0,6dB/km; SM(1550nm)-0,21dB/km,
- temperatur pracy -40°C do +70°C,
- gwarancja producenta min 25 lat,
- powłoka kabla LSOH,
- zakończenie na przełącznicy 1U, 19” kolor czarny,
- złącza minimum 12xLC simplex/duplex.

1.2.9 Klimatyzacja pomieszczenia serwerowni podstawowej.

W celu zapewnienia odpowiednich warunków temperaturowych pracy urządzeń w serwerowni należy dostarczyć, zamontować i uruchomić nowe klimatyzator.
Należy przewidzieć i dobrać klimatyzator typu split do montażu naściennego pracujących na powietrzu obiegowym dopasowanych do wydatków ciepła wydzielanych w pomieszczeniu serwerowni.
Podstawowe parametry klimatyzatora:

- Czynnik chłodniczy R-32,
- Przystosowane do chłodzenia przy niskich temperaturach zewnętrznych (podgrzewanie karteru sprężarki i regulator obrotów wentylatora skraplacza),
- Inwerter w sposób ciągły dostosowuje prędkość obrotową sprężarki do rzeczywistego obciążenia,
- Moc chłodnicza nominalna min. 3,5 kW,
- Klasa energetyczna A+++ (dla chłodzenia)
- Typ sprężarki DC INVERTER
- Zainstalowany moduł Wi-Fi
- Pilot zdalnego sterowania bezprzewodowy, możliwość podłączenia pilota przewodowego (panel sterowania).

1.2.10 Zabezpieczenia techniczne w pomieszczeniu serwerowni

W celu zabezpieczenia technicznego pomieszczenia serwerowni należy dostarczyć i uruchomić poniższe systemy bezpieczeństwa:

- system sygnalizacji włamania i napadu,
- system kontroli dostępu,
- system telewizji dozorowej,

W ramach wykonania systemów należy przeprowadzić następujące analizy:

- analiza zagrożeń,
- klasy systemu alarmowego,
- zasilania poszczególnych systemów i czasów podtrzymania bez zasilania podstawowego 230VAC.

Projekt wykonawczy systemu zabezpieczeń elektronicznych strefy serwerowni zostanie przygotowany w oparciu o następujące założenia i uzgodnienia z przedstawicielami Zamawiającego:

- zaprojektowane systemy mają wykrywać zdarzenia takie jak: włamanie, nieautoryzowane wejście, pożar, zalanie, napad,
- systemy: sygnalizacji włamania i napadu, kontroli dostępu, telewizji dozorowej mogą być rozbudową istniejących na obiekcie systemów, lub systemami autonomicznymi,
- główne urządzenia systemów zabezpieczeń elektronicznych będą zainstalowane wewnątrz pomieszczenia (strefy zabezpieczonej),
- system kontroli dostępu będzie składał się z: kontrolera SKD (kontroler z pamięcią uprawnień i funkcją anti-passback) czytnika wejściowego i wyjściowego (z historią), przycisku wyjścia awaryjnego, zwory elektromagnetycznej/elektrozaczepu, zasilacza buforowego,
- pomieszczenie serwerowni będzie odrębną strefą w systemie SSWiN,
- załączanie/wyłączanie systemu sygnalizacji włamania i napadu będzie przy drzwiach wejściowych do pomieszczenia z poziomu klawiatury LCD,
- sygnalizator akustyczno-optyczny będzie zainstalowany nad drzwiami wejściowymi do pomieszczenia,
- kamera w technologii IP, minimum 2Mpx, kompatybilna z istniejącym systemem na obiekcie, oświetlacz podczerwieni, obiektyw 2,8mm, obraz z kamery będzie dostępny u wskazanego administratora obiektu na istniejącym monitorze i będzie zapisywany na

dysku istniejącego rejestratora DVR lub lokalnej karcie pamięci kamery przez okres min. 30 dni.

Systemy zabezpieczeń powinny zaprojektować i wykonać pracownicy posiadający ważne legitymacje kwalifikowanego pracownika zabezpieczenia technicznego. Po wykonaniu systemów, przed przekazaniem do użytkowania należy przeprowadzić testy działania poszczególnych systemów i sporządzić protokół.

1.2.11 System monitorowania środowiska pracy w serwerowni

W ramach zadania należy dostarczyć i uruchomić systemu monitorowania parametrów środowiskowych pomieszczeń serwerowni. Pomieszczenie serwerowni będzie objęte systemem monitorowania stanów serwerowni. W tym celu należy zaprojektować moduły wykonawcze oraz centralę zbierającą sygnały.

W każdej lokalizacji monitoringiem systemu nadzoru objęte zostaną następujące sygnały:

- temperatura,
- wilgotność,
- otwarcie szafy, kontrola otwarcia drzwi,
- czujnik dymu,
- monitorowanie wycieków i zalania.

Urządzenie systemu monitoringu (centrala zbierająca sygnały) należy zainstalować w szafie serwerowej. Zarządzanie systemem nadzoru odbywać się będzie się z poziomu komputera PC, na którym należy uruchomić oprogramowanie systemu nadzoru. System monitorowania powinien posiadać interfejs sieciowy oraz wbudowane serwery wbudowane serwery HTTP, HTTPS, SNMP v1, 2c, 3, SMTP, Radius, Syslog, FTP, DHCP, Watchdog.

Czujniki do detekcji dymu, temperatury i wilgotności, wewnątrz pomieszczenia serwerowni powinny spełniać podstawowe parametry:

- pomiar temperatury w zakresie −10… +80°C,
- pomiar wilgotności 0 - 0.. 95% RH.

1.2.12 Urządzenia aktywne wymagania

Serwery wraz z oprogramowaniem

Dostarczone urządzenia serwerowe wraz z oprogramowaniem powinny być zainstalowane, uruchomione oraz powinny spełnić minimum poniższe parametry:

Obudowa:

- Obudowa Rack o wysokości max 2U. Możliwość instalacji minimum 12 dysków 3.5". Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
- Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.

Płyta główna:

- Płyta główna z możliwością zainstalowania do dwóch procesorów 3rd Generacji Intel Xeon.
- Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

Chipset:

- Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.

Procesor:

- Zainstalowane dwa procesory min. 8-rdzeniowe klasy x86, min. 2.8GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 131 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.

RAM:

- Minimum 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci,

- Płyta główna powinna obsługiwać do 8TB pamięci RAM.

Funkcjonalność pamięci RAM:

- Advanced ECC,
- Memory Page Retire,
- Fault Resilient Memory,
- Memory Self-Healing lub PPR,
- Partial Cache Line Sparing,

Gniazda PCI:

- Min. 4 sloty PCIe generacji 4

Interfejsy sieciowe/FC/SAS:

- Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ (porty nie mogą zostać osiągnięte poprzez karty w slotach PCIe).

Dyski twarde:

- Możliwość instalacji dysków SAS, SATA, SSD,
- Zainstalowane 2 dyski SSD SATA o pojemności min. 480GB, 6Gb, Hot-Plug,
- Zainstalowane 2 dyski SATA o pojemności min. 2TB, 6Gb, Hot-Plug,
- Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1,
- Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.

Kontroler RAID:

- Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache,
- Możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60,
- Wsparcie dla dysków samoszyfrujących.

Wbudowane porty:

- 5x USB, w tym min. 2 porty USB 3.0,
- 1 port VGA,
- Możliwość rozbudowy o Serial Port.

Video:

- Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024.

Wentylatory:

- Redundantne.

Zasilacze:

- Redundantne, Hot-Plug min. 800W każdy.

System operacyjny/dodatkowe oprogramowani

- Wirtualizacja Windows Server 2022 Standard wraz z licencjami dostępowymi.
- Należy dostarczyć nośnik umożliwiający downgrade do wersji Windows Server 2019 Standard

Bezpieczeństwo:

- Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych,
- Możliwość wyłączenia w BIOS funkcji przycisku zasilania,
- BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła ,
- Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
- Moduł TPM 2.0 ,
- Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera,
- Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.

Diagnostyka:

- Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.

Karta Zarządzania:

Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:

- zdalny dostęp do graficznego interfejsu Web karty zarządzającej,
- zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera),
- szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika,
- możliwość podmontowania zdalnych wirtualnych napędów,
- wirtualną konsolę z dostępem do myszy, klawiatury,
- wsparcie dla IPv6,
- wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish,
- możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer,
- możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer,
- integracja z Active Directory,
- możliwość obsługi przez dwóch administratorów jednocześnie
- wsparcie dla dynamic DNS,
- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej,
- możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera,
- możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera.

Certyfikaty

- Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001
- Serwer musi posiadać deklaracja CE,

- Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.

Warunki gwarancji:

- 3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta,
- Możliwość rozszerzenia gwarancji przez producenta do 7 lat,
- Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.

Dokumentacja użytkownika:

- Zamawiający wymaga dokumentacji w języku polskim lub angielskim,
- Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bez.

Przełączniki sieciowe

W punktach dystrybucji głównym i pośrednim zainstalować należy przełączniki sieciowe umożliwiające obsługę wszystkich urządzeń w sieci. W celu konfiguracji i podziału logicznego sieci w obrębie VLAN należy przeprowadzić audyt i inwentaryzacje i uzgodnić z użytkownikiem.

Parametry fizyczne platformy:

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U,
- Zasilanie AC 230V,
- Redundantny zasilacz,
- Maksymalny pobór mocy: max 48 W,
- Minimalny zakres temperatury pracy: 0-50^{o}C,

Interfejsy sieciowe - wymagania minimalne:

- Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
  a) 48 porty GE, RJ-45.
  b) 4 porty 10 GE SFP+.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 176 Gbps,
- Liczba pakietów na sekundę min. 260 Mpps,
- Tablica adresów MAC o pojemności co najmniej 32 k wpisów,
- Opóźnienie wprowadzane przez przełącznik - poniżej 1 mikrosekund,
- Bufor Pakietów 2 MB,

Zarządzanie:

- Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania,
- Wbudowany 1 port konsoli szeregowej do pełnego zarządzania,
- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS),
- Wsparcie dla SNMP w wersjach 1-3,
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami,
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI,
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline,
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP),
- •Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+,
- Automatycznie wykonywane rewizje konfiguracji,

Wymagane funkcje:

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń,
- Obsługa Jumbo Frames,

- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree),
- Agregacja portów zgodna ze standardem 802.3ad,
- Obsługa co najmniej 4000 VLANów, zgodna ze standardem 802.1Q,
- Wsparcie dla Private VLAN,
- Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP,
- Port-mirroring,
- Uwierzytelnianie 802.1x na poziomie portu,
- Uwierzytelnianie 802.1x w oparciu o adres MAC,
- W ramach 802.1x wsparcie dla dedykowanego VLANu dla gości (guest VLAN),
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN,
- Obsługa routingu statycznego,

Gwarancja oraz wsparcie:
System musi być objęty serwisem gwarancyjnym producenta przez okres [36] miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Urządzenie UTM

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.

Redundancja, monitoring i wykrywanie awarii:

- 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.
- Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych,
- Monitoring stanu realizowanych połączeń VPN.

Interfejsy, Dysk, Zasilanie,Montaż:

- System realizujący funkcję Firewall musi dysponować minimum:
    - 10 portami Gigabit Ethernet RJ-45,
    - 2 gniazdami SFP 1 Gbps.
- System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB,
- Wymagane zasilanie z AC 240V, 50Hz,
- Montażu w szafie rack 19”, 1U bezpośrednio lub przy pomocy dedykowanego zestawu.

Parametry wydajnościowe:

- W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę,
- Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B,
- Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps,
- Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps,
- Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps,
- Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps,

- Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.
-

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:

- Kontrola dostępu - zapora ogniowa klasy Stateful Inspection,
- Kontrola Aplikacji,
- Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN,
- Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS,
- Ochrona przed atakami - Intrusion Prevention System,
- Kontrola stron WWW,
- Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3,
- Zarządzanie pasmem (QoS, Traffic shaping),
- Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)
- 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,
- Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2,
- 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.

Polityki, Firewall:

- Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń,
- System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

- Translację jeden do jeden oraz jeden do wielu,

- Dedykowany ALG (Application Level Gateway) dla protokołu SIP,
- W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN,
- Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików,
- 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.

Połączenia VPN:

- System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
- Wsparcie dla IKE v1 oraz v2.
- Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
- Obsługa protokołu Diffie-Hellman grup 19 i 20.
- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
- Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling” dla połączeń Client-to-Site.
- 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.

Routing i obsługa łączy WAN:

- W zakresie routingu rozwiązanie powinno zapewniać obsługę:
- Routingu statycznego.
- Policy Based Routingu.
- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN:

- System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
- Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem:

- System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
- Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
- System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware:

- Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
- System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
- System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
- 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.

- System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
- Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami:

- Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
- System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
- Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
- System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
- 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.
- Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji:

- Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
- Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
- Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
- Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

- Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

- 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.
- Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
- Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
- Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
- Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
- W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

- System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
- Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
- Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.

Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

- 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.
- Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

- Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
- System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
- System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
- 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.

Logowanie:

- 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.
- Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
- Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty:

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje:

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

- Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres [36] miesięcy.

Gwarancja oraz wsparcie:

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres [36] miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

1.2.13 Okablowanie strukturalne obiektu

W budynku UM Łapy przy ul. Sikorskiego 24 wykonać należy nową dedykowaną sieć teleinformatyczną w postaci okablowania strukturalnego wraz z zakończeniami w postaci modułów gniazd logicznych i paneli krosowych w punktach dystrybucji. Zakłada że instalacja okablowania strukturalnego wykonana zostanie w oparciu o topologię gwiazdy. Topologicznie sieć składa się z dwóch punktów dystrybucji, Główny punkt dystrybucji zlokalizowany w serwerowni i pośredni punkt dystrybucji w jednym z pomieszczeń na wyższej kondygnacji. Trasy i sposób ułożenia kabli oraz dokładne rozmieszczenie gniazd logicznych na terenie budynku należy ustalić na etapie projektowym. Dokumentację projektową wykonawczą sieci wykonać należy w uzgodnieniu z inwestorem, wszystkie przyjęte rozwiązania i sposób prowadzenia prac przed przystąpieniem do ich wykonania powinny być zatwierdzone przez Zleceniodawcę.

Dokumentacja wykonawcza i powykonawcza sieci strukturalnej.

Dokumentacja w zakresie sieci strukturalnej powinna spełniać ogólne założenia opisane w punkcie 1.2 niniejszego PFU oraz poniższe wymagania. Dokumentacja powykonawcza sieci strukturalnej powinna być wydzielonym dokumentem umożliwiającym funkcjonalną obsługę sieci strukturalnej obiektu.

W ramach dokumentacji i opracowania projektu wykonawczego a następnie wykonania prac instalacyjnych należy:

- przeprowadzić kompleksową inwentaryzację stanu istniejącego i bieżącej infrastruktury w obiekcie,
- rozpoznać i zaplanować trasy prowadzenia okablowania strukturalnego,
- sporządzenie planu rozmieszczenia punktów logicznych,
- sporządzenie planu zakończenia kabli w punktach dystrybucji (serwerownia główna i punkty pośrednie),

- sporządzić i zatwierdzić u Zamawiającego harmonogram realizacji prac w uwzględnieniem bieżącego funkcjonowania urzędu i jednostek podległych,
- rozwiązania techniczne, deklaracje i dopuszczenia do obrotu zastosowanych materiałów i urządzeń oraz sposób certyfikacji należy przedłożyć do zatwierdzenia zamawiającemu,

Dokumentacja powykonawcza oprócz zmian powykonawczych naniesionych w odniesieniu do dokumentacji projektowej powinna zawierać część pomiarową potwierdzającą spełnienie zakładanych parametrów okablowania.

Zakres i kolejność prowadzenia prac

Po uzyskaniu akceptacji rozwiązań projektowych zawartych w dokumentacji wykonawczej w raz z przedstawionym harmonogramem należy przeprowadzić poniższe prace:

- demontaż lub przesunięcie istniejących gniazd kablowych (o ile zakłada to rozwiązanie projektowe),
- budowa i wykonanie docelowych tras kablowych wraz z modernizacja istniejących tras kablowych w postaci koryt kablowych, drabin, przejąć pionowych pomiędzy kondygnacjami,
- ułożenie okablowania sieci strukturalnej,
- zakończenie linii kablowych na modułach w punktach rozdziału,
- zakończenie linii kablowych w modułach gniazd naściennych,
- oznakowanie okablowania i modułów rozdziału i zakończenia sieci,
- wykonanie pomiarów odbiorczych sieci strukturalnej,
- przyłączenie kabli krosowych i przepięcie urządzeń sieciowych zgodnie z harmonogramem,
- wykonanie dokumentacji powykonawczej i pomiarowej.

Prowadzenie kabli

Sposób układania kabli w budynku musi uwzględniać położenie innych instalacji istniejących w budynku w szczególności emitujących zakłócenia elektroenergetyczne i istniejące okablowanie strukturalne. Sposób ułożenia okablowania powinien spełniać zalecani producenta oraz wymagania w zakresie maksymalnych odległości od punktu rozdziału do gniazd przyłączeniowych (nie większe

niż 90m) oraz pozostałe zalecenia producenta okablowania. Okablowanie należy układać w istniejących kanałach kablowych (o ile wystarczająca przestrzeń w korycie), nowobudowanych korytach PVC oraz w przestrzeni nadsufitowej. Nie planuje się układania kabli wewnątrz ścian i w tynku.
W nowobudowanych odcinkach koryt kablowych należy pozostawić rezerwę min 30% wypełnienia celem przyszłej rozbudowy i bieżącego użytkowania obiektu. W pomieszczeniu serwerowni kable układać należy na drabinie kablowej.
Sposób rozprowadzania okablowania opisany jest w dokumencie normalizacyjnym EIA/TIA – 569 specyfikującym między innymi:

- instalację podstropową;
- trakty naścienne;
- rurarz;
- rurarz pionowy;
- instalację podwieszaną.

Długość łącza stałego (permanent link) okablowania strukturalnego, tj. odległość pomiędzy złączem RJ45 w PL a złączem RJ45 w patch-panelu po stronie punktu dystrybucyjnego, nie może przekroczyć 90 metrów. Kabel przyłączeniowy od strony gniazda jak i szafy, nie może przekroczyć długości 5 metrów, jeśli wykorzystano maksymalną długość łącza stałego. Całość łącza z okablowaniem szafowym oraz okablowaniem obszaru roboczego, czyli kanał, nie może w sumie przekroczyć 100 metrów. Podczas instalacji należy pamiętać o odpowiednich promieniach gięcia kabla. Instalacja ze zbyt niskim promieniem gięcia kabla może doprowadzić do pogorszenia właściwości transmisyjnych w torze.
Okablowanie powinno być ciągłe na całej długości toru bez złącz i spawów od stanowiska roboczego do panelu rozdzielczego. Określając trasy dla kabli logicznych uwzględniono konstrukcję budynku oraz bezkolizyjność z innymi instalacjami i urządzeniami; trasa przebiega wzdłuż linii prostych równoległych i prostopadłych do ścian i stropów zmieniając swój kierunek tylko w zależności od potrzeb (tynki, rozgałęzienia, podejścia do urządzeń), trasa przebiegu jest przy tym łatwo dostępna do konserwacji i remontów, a jej wytyczanie uwzględnia miejsca mocowania konstrukcji wsporczych instalacji.

Przy realizacji tras kablowych pod potrzeby okablowania należy wziąć pod uwagę wymagania normy PN-EN 50174-2:2010/A1:2011 dotyczące równoległego prowadzenia różnych instalacji w budynku, m.in. instalacji zasilającej i zapewnić odpowiednie odległości pomiędzy okablowaniem.

Sieć strukturalna pełnić będzie funkcję okablowania dla potrzeb:

- transmisja danych, sieci LAN dla potrzeb własnych,
- instalacji telefonicznej (np. VoIP, ISDN),
- okablowania dla potrzeb instalacji teletechnicznych (np. CCTV, SSWiN, KD, IPTV).

Wykonane okablowanie strukturalne musi spełniać następujące warunki:

- Wszystkie komponenty systemu okablowania mają być zgodne z wymaganiami obowiązujących norm wg.:
  - ISO/IEC 11801,
  - EN 50173-1,
  - ANSI/TIA/EIA 568-C.2.
- Okablowanie w obiekcie, wykonane będzie jako nie/ekranowana sieć okablowania strukturalnego klasy EA (komponenty minimum kategorii 6A), poprowadzona kablem o paśmie przenoszenia minimum 700 MHz. Konstrukcja kabla pozwalająca osiągnąć wysokie parametry transmisyjne oraz zmniejszyć przesłuchy NEXT i PSNEXT oraz zmniejszenie przesłuchów obcych Alien Crosstalk. Kabel musi spełniać wymagania stawiane komponentom przez najnowsze normy,
- Ilość i lokalizację gniazd oraz punktów dystrybucyjnych przyjęto na podstawie aktualnych, dla daty wykonywania dokumentacji, wytycznych Użytkownika i bieżącej aranżacji wnętrz. Ostateczna i precyzyjna lokalizacja gniazd logicznych powinna być ustalona między Użytkownikiem, a Wykonawcą w trakcie realizacji,
- Wymagane jest aby okablowanie i osprzęt pochodził od jednego dostawcy systemu okablowania strukturalnego i powinien być objęte jednolitą i spójną gwarancją na okres minimum 25 lat obejmując wszystkie elementy pasywne toru transmisyjnego,
- Wszystkie elementy pasywne składające się na okablowanie strukturalne muszą pochodzić z oferty reprezentującej system okablowania w takim zakresie, aby zostały spełnione warunki niezbędne do uzyskania wystawionego przez producenta bezpłatnego Certyfikatu Okablowania Strukturalnego oraz udzielenie 25-letniej gwarancji.

1.2.14 Okablowanie

Stosować należy kabel kat. 6A o konstrukcji U/FTP (kabel ekranowany). Minimalne wymagania elementów okablowania strukturalnego to kategoria 6A (komponenty) / Klasa EA (wydajność całego systemu).
Kabel powinien spełniać wymagania poniższych norm:

- EN 50173-1:2018-07
- ISO/IEC 11801 Edition 2.2
- ANSI/TIA-568-C.0/C.1/C.2
- IEC 60754-2
- IEC 60332-1

Do każdego portu RJ45 punktu logicznego należy doprowadzić kabel skrętkowy 4-parowy, który należy rozprowadzić zgodnie z zaprojektowanymi i uzgodnionymi z użytkownikiem trasami. .Każdy kabel skrętkowy, należy zakończyć na pojedynczym module RJ45 (gnieździe RJ45). Nie dopuszcza się rozdziału jednego kabla 4-parowego na większą ilość portów (nie dopuszcza się wkładek i przejściówek rozdzielających). Każdy kabel powinien mieć trwałe oznaczenie na dwóch końcach przy zakończonych modułach wg przyjętego systemu numeracji.
Ze względu na przyjęte wymiary przepustów kablowych oraz zaprojektowane trakty prowadzenia kabli i związane z tym prześwity, wymagane jest zastosowanie medium transmisyjnego o maksymalnej średnicy zewnętrznej 7,5mm. Nie dopuszcza się kabli o większej średnicy zewnętrznej. Kabel ten ma zapewniać pozytywne parametry transmisyjne w całym paśmie minimum 700MHz. Projektowany kabel musi posiadać zewnętrzną powłokę LSOH nie wydzielającą szkodliwych toksyn podczas spalania. Wymaga się, aby kabel posiadał euroklasę min. Dca s2, d0, a1 zgodnie z dyrektywą CPR.

Minimalne wymagania wobec kabla:

Budowa:	U/FTP (kabel ekranowany)
Rodzaj powłoki:	LSOH (Low Smoke Zero Halogen)
Specyfikacje:	ISO/IEC 11801, EN 50173,TIA 568A, TIA/EIA 854
Średnica przewodnika:	23AWG
Średnica zewnętrzna kabla:	max. 7,5±0,2mm

Częstotliwość pracy:	700 MHz
NPV:	77%(0,77)

1.2.15 Moduły i aparatura

Panele krosowe

Okablowanie zakończyć należy w szafach w punktach dystrybucyjnych na panelach modułowych. Panele rozdzielcze powinny umożliwiać wpinanie 24 modułów RJ45 typu keystone, takich samych jak w gniazdach abonenckich. Panele modularne w odróżnieniu do paneli ze zintegrowaną płytką PCB pozwala na szybszą i łatwiejszą (w razie potrzeby czy awarii) wymianę jednego gniazda.
Panel powinien posiadać 24 porty i wysokość 1U. Panel musi posiadać zintegrowaną prowadnicę kabli przychodzących, co zapewni swobodne uchwycenie kabli i eliminacje naprężeń związanych z wagą doprowadzonych kabli. Ponad to panel musi być oznaczony logo producenta zastosowanego okablowania. Patchpanel musi być wyposażony w gwintowane przyłącze linki uziemienia panela. Wszystkie zainstalowane panele muszą być podłączone poprzez ww. przyłącze do szyny uziemienia szafy.

Moduły RJ45

Punkty logiczne należy wykonać w oparciu o ekranowane moduły typu keystone kategorii 6A mocowane w odpowiednich adapterach dopasowanych do osprzętu elektroinstalacyjnego.
Moduł musi spełniać wymagania kategorii 6A (klasy EA) wg poniższych norm:

- EN 50173-1:2018-07
- EN 50173-1:2011
- ISO/IEC 11801 Edition 2.2
- ANSI/TIA-568-C.0
- ANSI/TIA-568-C.1
- ANSI/TIA-568-C.2
- IEC 60603-7

Zgodność modułu RJ45 z powyższymi normami musi zostać potwierdzona certyfikatem niezależnego laboratorium badawczego (np. DELTA Force Technology).

Należy użyć modułów zarabianych beznarzędziowo. Maksymalny rozplot pary transmisyjnej nie może być większy niż 6mm od złącza. Moduł RJ45 kat. 6A powinien posiadać zintegrowaną klapkę

przeciwkurzową, dzięki czemu zapewniona jest szczelność, gdy gniazdo jest nieużywane. Chroni ona piny przed zakurzeniem, dzięki czemu występuje mniejsze prawdopodobieństwo wytworzenia łuków elektrycznych przy wpinaniu gdy zasilanie jest prowadzone przez skrętkę (PoE).

Moduł musi być zgodny ze standardem Keystone. Złącza IDC modułów powinny mieć możliwość podłączenia żył o AWG 23-26. Moduł powinien posiadać oznaczenia kolorystyczne ułatwiające przyłączenie kabla w sekwencji 568B lub 568A.

Minimalne wymagania modułów RJ45:

Budowa:	Dostosowana do rozszycia kabla U/FTP, zarobienie beznarzędziowe, typu butterfly
Zabezpieczenie:	Klapka przeciwkurzowa, samozamykająca się
Obsługa PoE	PoE, PoE+, 4PPoE, Power over HDBase-T
Częstotliwość:	500MHz
Średnica przewodnika:	Od 24 do 22 AWG
Trwałosć:	min. 1000 wpięć/wypięć
Powłoka pinów:	Złoto o grubości 1,25 μm

Punkty logiczne PL (gniazda przyłączeniowe użytkowników) należy zorganizować w postaci modułów RJ45 keystone montowanych w adapterze z tworzywa sztucznego o wymiarach 45x45mm (format Mosaic). Ten uniwersalny standard montażowy zapewni organizację punktów elektryczno-logicznych w zależności od potrzeb - w formie natynkowej lub podtynkowej. W zależności od lokalnych potrzeb możliwe są poniższe aranżacje punktów logicznych:

- Podwójny punkt logiczny PL (2xRJ45)
- Poczwórny punkt logiczny 2xPL (4xRJ45)
- Pojedynczy punkt logiczny PL(1xRJ45)

W celu łatwego zarządzania okablowaniem strukturalnym każdy moduł RJ45 w punkcie logicznym musi posiadać oznaczanie jednoznacznie je identyfikujące.

1.2.16 Pomiary i testy okablowania

Pomiary i testy okablowania miedzianego

Po zakończeniu prac instalację należy poddać pomiarom i badaniom sprawdzającym. Wykonane pomiary powinno być zgodne z normą PN-EN 50346:2004/A1+A2:2009. Pomiary należy wykonać dla wszystkich interfejsów okablowania poziomego oraz szkieletowego. Należy użyć miernika dynamicznego (analizatora), który posiada wgrane oprogramowanie umożliwiające pomiar parametrów według aktualnie obowiązujących norm. Sprzęt pomiarowy musi posiadać aktualny certyfikat potwierdzający dokładność jego wskazań. Analizator okablowania wykorzystany do pomiarów musi charakteryzować się przynajmniej V klasą dokładności wg IEC 61935-1/Ed. 3 (proponowane urządzenia to np. FLUKE DSX 5000). W przypadku sieci miedzianej bez użycia kabli krosowych pomiary należy wykonać w konfiguracji pomiarowej łącza stałego (ang. „Permanent Link") – przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego. W przypadku użycia kabli krosowych pomiary należy wykonać w konfiguracji pomiarowej kanału razem z kablami krosowymi (ang. „Channel") – przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego. Kable krosowe, które zostały użyte do przeprowadzenia pomiarów należy przekazać Inwestorowi.

Wymagane parametry testu dla kabli miedzianych:

- Wire Map mapa połączeń,
- Length długość (m),
- Propagation delay opóźnienie propagacji (ns/m),
- Delay skew rozrzut opóźnienia,
- Attenuation/Insertion loss tłumienie (dB),
- Return Loss tłumienność odbicia (dB),
- NEXT przesłuch zbliżny (dB),
- PS NEXT suma przesłuchów zbliżnych,
- FEXT przesłuch zdalny (dB),
- ACR stosunek tłumienności do NEXT,

Pomiary połączeń światłowodowych

Pomiary sieci światłowodowej powinny być wykonane zgodnie z normą PN-EN 14763-3:2009/A1:2010. Należy przeprowadzić pomiary dwukierunkowe, w których źródło świetlnego sygnału referencyjnego będzie umieszczone w pierwszym kroku na jednym końcu łącza, a w kolejnym kroku na drugim końcu łącza.

Łącza wielomodowe (MM) należy przetestować w dwóch oknach transmisyjnych, dla długości fali: 850 nm i 1300 nm. Łącza jednomodowe (SM) należy przetestować w dwóch oknach transmisyjnych, dla długości fali: 1310 nm i 1550 nm.

Należy wykonać pomiary certyfikacyjne, w których po zmierzeniu rzeczywistych wartości parametrów łącza, miernik automatycznie porówna je z granicznymi wartościami definiowanymi przez aktualne normy okablowania i określi wynik porównania. Wyniki pomiarów certyfikacyjnych wszystkich łączy musza być prawidłowe.

Wymagany zakres mierzonych parametrów:

- Ciągłość łącza,
- Długość łącza,
- Tłumienie włókien dla dwóch długości fali,
- Test tłumienności i parametru,
- Return loss zestawem OCTS o dokładności +/- 0.2dB lub lepszej z dwóch stron każdego kabla, w dwóch oknach optycznych 850nm i 1300nm.

1.2.17 Gwarancje na okablowania

Całość rozwiązania ma być objęta jednolitą, spójną 25-letnią gwarancją systemową producenta. Gwarancja musi być udzielona klientowi końcowemu bezpośrednio przez producenta, a nie od dystrybutora okablowania.

Gwarancja systemowa ma obejmować:

- gwarancję systemową (Producent zagwarantuje, że jeśli w jego produktach podczas dostawy, instalacji bądź 25-letniej eksploatacji wykryte zostaną wady lub usterki fabryczne, to produkty te zostaną naprawione bądź wymienione),

- gwarancję parametrów łącza/kanału (Producent zagwarantuje, że łącze stałe bądź kanał transmisyjny zbudowany z jego komponentów prze okres 25 lat będzie charakteryzował się parametrami transmisyjnymi przewyższającymi wymogi stawiane przez normę ISO/IEC 11801:2002/Am2: 2010 dla okablowania klasy EA).
- gwarancję aplikacji (Producent zagwarantuje, że na jego systemie okablowania przez okres 25 lat będą pracowały dowolne aplikacje (współczesne i stworzone w przyszłości), które zaprojektowane były (lub będą) dla systemów okablowania klasy EA (w rozumieniu normy ISO/IEC 11801 2nd edition:2010).

2. Część informacyjna

2.1 Dokumenty potwierdzające zgodność zamierzenia budowlanego z wymaganiami wynikającymi z odrębnych przepisów

Wszystkie dokumenty potwierdzające zgodność zamierzenia budowlanego z wymaganiami wynikającymi z odrębnych przepisów oraz inne uzgodnienia niezbędne do realizacji przedmiotu zamówienia Wykonawca powinien uzyskać na etapie realizacji projektu, w fazie projektowej.

2.2 Oświadczenie Zamawiającego stwierdzające prawo do dysponowania nieruchomościami

Zamawiający oświadcza iż posiada prawo do dysponowania nieruchomością na cele przedmiotowej inwestycji. W przypadku konieczności uzyskania dodatkowych zgód i zezwoleń Wykonawca uzyska je w własnym zakresie na etapie wykonywania projektu budowlano-wykonawczego.

2.3 Inwentaryzacja lub dokumentacja obiektów budowlanych

Zamawiający nie przewiduje przebudowy, odbudowy, rozbudowy lub rozbiórki obiektów budowlanych w zakresie architektury i konstrukcji. Instalacja urządzeń aktywnych nie zmieni dotychczasowej funkcji pomieszczeń. Jeżeli na etapie wykonania projektu budowlano-wykonawczego okaże się to niezbędne wówczas Wykonawca o ile będzie to konieczne z punktu widzenia prawa budowlanego przygotuje niezbędną inwentaryzację i dokumentację.

2.4 Przepisy prawne i normy związane z projektowaniem i wykonaniem zamierzenia budowlanego

W ramach niniejszego projektu należy zachować kolejność stosowania wytycznych, norm rozporządzeń i zarządzeń wymienionych w dokumentach:

- umowa wykonawcza,
- program Funkcjonalno-Użytkowy,
- w przypadku braku specyfikacji w wyżej wymienionych dokumentach należy przyjąć wymagania co do prac i materiałów zgodnie z załączoną listą norm i rozporządzeń;
- w przypadku wymagań równoległych należy stosować rozwiązanie o parametrach bardziej korzystnych z punktu widzenia Zamawiającego i przedmiotu zamówienia.

Zastosowanie mają przepisy i normy:

- PN-EN 60529 Stopnie ochrony zapewniane przez obudowy (Kod IP),
- EIA/TIA 568 Standardy okablowania budynków wg ANSI,
- PN-EN 50173 Technika informatyczna – systemy okablowania strukturalnego,
- PN-EN 50174 Technika informatyczna. Instalacja okablowania strukturalnego,
- PN-EN 50346 Technika informatyczna Instalacja okablowania – Badanie zainstalowanego okablowania,
- PN-EN 62676-1-1:2014-06E Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 1-1: Wymagania systemowe -- Postanowienia ogólne,
- PN-EN 62676-1-2:2014-06E Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 1-2: Wymagania systemowe -- Wymagania eksploatacyjne dotyczące transmisji wizji,
- PN-ISO/IEC 2382 Technika informatyczna – Terminologia,
- PN-IEC 60364-4-482 Instalacje elektryczne w obiektach budowlanych. Ochrona dla zapewnienia bezpieczeństwa. Dobór środków ochrony w zależności od wpływów zewnętrznych. Ochrona przeciwporażeniowa,
- PN-HD 60364-4-41:2017-09 – Instalacje elektryczne niskiego napięcia – Część 4-41: Ochrona dla zapewnienia bezpieczeństwa – Ochrona przed porażeniem elektrycznym,

- PN-HD 60364-5-534:2016-04 - Instalacje elektryczne niskiego napięcia -- Część 5-534: Dobór i montaż wyposażenia elektrycznego -- Odłączanie izolacyjne, łączenie i sterowanie -- Urządzenia do ochrony przed przejściowymi przepięciami,
- PN-IEC 60364-7-707:1999 - Instalacje elektryczne w obiektach budowlanych. Wymagania dotyczące specjalnych instalacji lub lokalizacji. Wymagania dotyczące uziemień instalacji urządzeń przetwarzania danych,
- PN-HD 60364-1:2010 - Instalacje elektryczne niskiego napięcia Część:1 Wymagania podstawowe, ustalanie ogólnych charakterystyk, definicje,
- PN-IEC 60364-5-52:2002 - Instalacje elektryczne w obiektach budowlanych. Dobór i montaż wyposażenia elektrycznego,
- PN-IEC 60364-5-534:2003 - Instalacje elektryczne w obiektach budowlanych. Dobór i montaż wyposażenia elektrycznego. Urządzenia do ochrony przed przepięciami,

Ustawy i rozporządzenia:

- Ustawa z dnia 7 lipca 1994 roku Prawo Budowlane (Dz. U. 2006, Nr 156, poz. 1118, zpóźniejszymi zmianami),
- Rozporządzenie Ministra Infrastruktury z dnia 3 lipca 2003 roku w sprawie szczegółowego zakresu i formy projektu budowlanego (Dz. U. 2003, Nr 120, poz. 1133, z późniejszymi zmianami);
- Rozporządzenie Ministra Infrastruktury z dnia 2 września 2004 roku w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego (Dz. U. 2004, Nr 202, poz. 2072, z późniejszymi zmianami),
- Rozporządzenie Ministra Infrastruktury z dnia 23 czerwca 2003 w sprawie informacji dotyczącej bezpieczeństwa ochrony zdrowia oraz planu bezpieczeństwa i ochrony zdrowia. (Dz. U. 2003, Nr 120, poz. 1126 z późniejszymi zmianami),

Wszystkie roboty należy wykonywać zgodnie z obowiązującymi normami i przepisami. Prace należy prowadzić zgodnie z obowiązującymi przepisami BHP i PPOŻ. W przypadku kiedy normy europejskie nie definiują konkretnych rozwiązań związanych z budową optotelekomunikacyjnej

kanalizacji kablowej, wówczas należy stosować polskie normy zakładowe i katalog dobrych praktyk.

2.5 Inne posiadane informacje, dokumenty i informacje niezbędne do zaprojektowania i prowadzenia robót budowlanych.

Wykonawca prac musi spełniać następujące warunki:

- posiada uprawnienia do wykonywania określonej działalności lub czynności, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień,
- posiadają niezbędną wiedzę i doświadczenie oraz potencjał techniczny, a także
- dysponuje osobami zdolnymi do wykonania zamówienia.

Wykonawca jest zobowiązany zrealizować przedmiot zamówienia spełniając wymagania ustawy Prawo budowlane, rozporządzenia Ministra Infrastruktury w sprawie warunków technicznych jakim powinny odpowiadać budynki i ich usytuowanie, innych ustaw i rozporządzeń, Polskich Norm, zasad wiedzy technicznej i sztuki budowlanej.

Zamawiający wymaga przedłożenia do akceptacji rysunków wykonawczych i szczegółowych specyfikacji technicznych wykonania i odbioru robót przed ich skierowaniem do realizacji, w aspekcie ich zgodności z ustaleniami programu funkcjonalno-użytkowego i umowy.

Zamówienie obejmuje kompletne wykonanie w/w instalacji, w tym m.in.: dostawę wszystkich materiałów montażowych i elementów składowych, przeprowadzenie testów. Wszelkie koszty materiałów i prac wymaganych do pełnego uruchomienia systemu (w tym estetycznego wykończenia), a nie wymienionych w opisie zamówienia, pokrywa Wykonawca.

Wykonawca odpowiedzialny jest za zapewnienie bezpieczeństwa na terenie miejsca robót, w szczególności należy opracować i zatwierdzić projekt organizacji ruchu na czas prowadzenia robót. Projekt wykona Wykonawca we własnym zakresie i własnym kosztem.

Wykonawca będzie zobowiązany do przyjęcia odpowiedzialności od następstw i za wyniki działalności w zakresie:

- organizacji robót budowlanych,
- zabezpieczenia interesów osób trzecich,
- warunków bezpieczeństwa i higieny pracy,
- warunków bezpieczeństwa ruchu drogowego,
- zabezpieczenia robót przed dostępem osób trzecich,

- zabezpieczenia terenu robót od następstw związanych z budową.

Na Wykonawcy spoczywa odpowiedzialność za takie zabezpieczenia materiałów i urządzeń, aby dotarły one na plac budowy w stanie nienaruszonym. Wszystkie materiały i urządzenia należy umieścić w opakowaniach i kontenerach odpowiedniej jakości, w taki sposób aby były one odporne na wszelkie uszkodzenia podczas ich transportu. Należy podjąć środki ostrożności w celu ochrony przed kontaktem z wilgotnym środowiskiem. Wykonawca będzie odpowiedzialny za rozładunek i składowanie materiałów/urządzeń.

Wszystkie Materiały przeznaczone do wykorzystania w ramach prowadzonej inwestycji będą materiałami w najwyższym stopniu nadającymi się do niniejszych Robót.

Wszystkie materiały i urządzenia zastosowane do wykonania robót powinny być:

- nowe,
- w najwyższym gatunku bieżąco produkowanym,
- odpowiadać wymaganiom norm i przepisów wymienionych w Dokumentacji Projektowej, opisie robót oraz innych nie wymienionych dokumentach, lecz zgodnych z obowiązującymi normami i przepisami,
- zgodne z polskimi przepisami, Ustawą o wyrobach budowlanych i świadectwami dopuszczenia do obrotu oraz posiadać wymagane certyfikaty bezpieczeństwa.

Zamawiający dopuści do użycia tylko te materiały które posiadają:

- Certyfikat na znak bezpieczeństwa, wskazujący, że zapewniono zgodność z kryteriami technicznymi określonymi na podstawie właściwych zharmonizowanych Polskich Norm, aprobat technicznych oraz właściwych przepisów i dokumentów technicznych.
- Deklarację zgodności lub certyfikat zgodności z :
  - zharmonizowaną Polską Normą
  - aprobatą techniczną, w przypadku wyrobów, dla których nie ustanowiono odpowiedniej normy, jeżeli nie są objęte certyfikacją i które spełniają wymogi specyfikacji technicznej.

Produkty przemysłowe muszą posiadać w/w dokumenty wydane przez producenta, a w razie potrzeby poparte wynikami badań wykonanych przez niego. Jakiekolwiek materiały, które nie spełniają tych wymagań będą odrzucone.

Zamawiający przewiduje bieżącą kontrolę wykonywanych prac objętych zamówieniem. Kontroli zamawiającego będą poddane w szczególności:

- rozwiązania projektowe zawarte w projekcie budowlanym przed złożeniem wniosku wykonawcy o wydanie pozwolenia na budowę oraz projekty wykonawcze i specyfikacje techniczne wykonania i odbioru robót, w aspekcie ich zgodności z programem funkcjonalno-użytkowym oraz warunkami umowy,
- stosowane gotowe wyroby budowlane, w odniesieniu do dokumentów potwierdzających ich dopuszczenie do obrotu oraz zgodności parametrów z danymi zawartymi w projektach wykonawczych i w specyfikacjach technicznych,
- sposób wykonania prac objętych zamówieniem w aspekcie zgodności wykonania z projektami wykonawczymi i specyfikacjami technicznymi, a w szczególności sposobu wykonania połączenia światłowodowego, punktów kamerowych, centrów monitoringu.

Zamawiający przewiduje ustanowienie osoby upoważnionej do zarządzania realizacją umowy odpowiedzialnego za:

- zapewnienie współpracy z wykonawcą,
- prowadzenie kontroli wykonywanych robót budowlanych,
- dokonywania odbiorów.

Roboty będą przyjęte przez Zamawiającego po ich zakończeniu z wynikiem pozytywnym prób końcowych. Wykonanie zobowiązań Wykonawcy potwierdza Zamawiający, bezusterkowym protokołem końcowym odbioru prac.

Wykonawca dostarczy instrukcje obsługi w języku polskim w formie papierowej i elektronicznej dla wszystkich zainstalowanych urządzeń. Wszelkie roszczenia osób i instytucji spowodowane zniszczeniami lub uszkodzeniami mienia, związanymi z wykonawstwem robót ponosi Wykonawca.

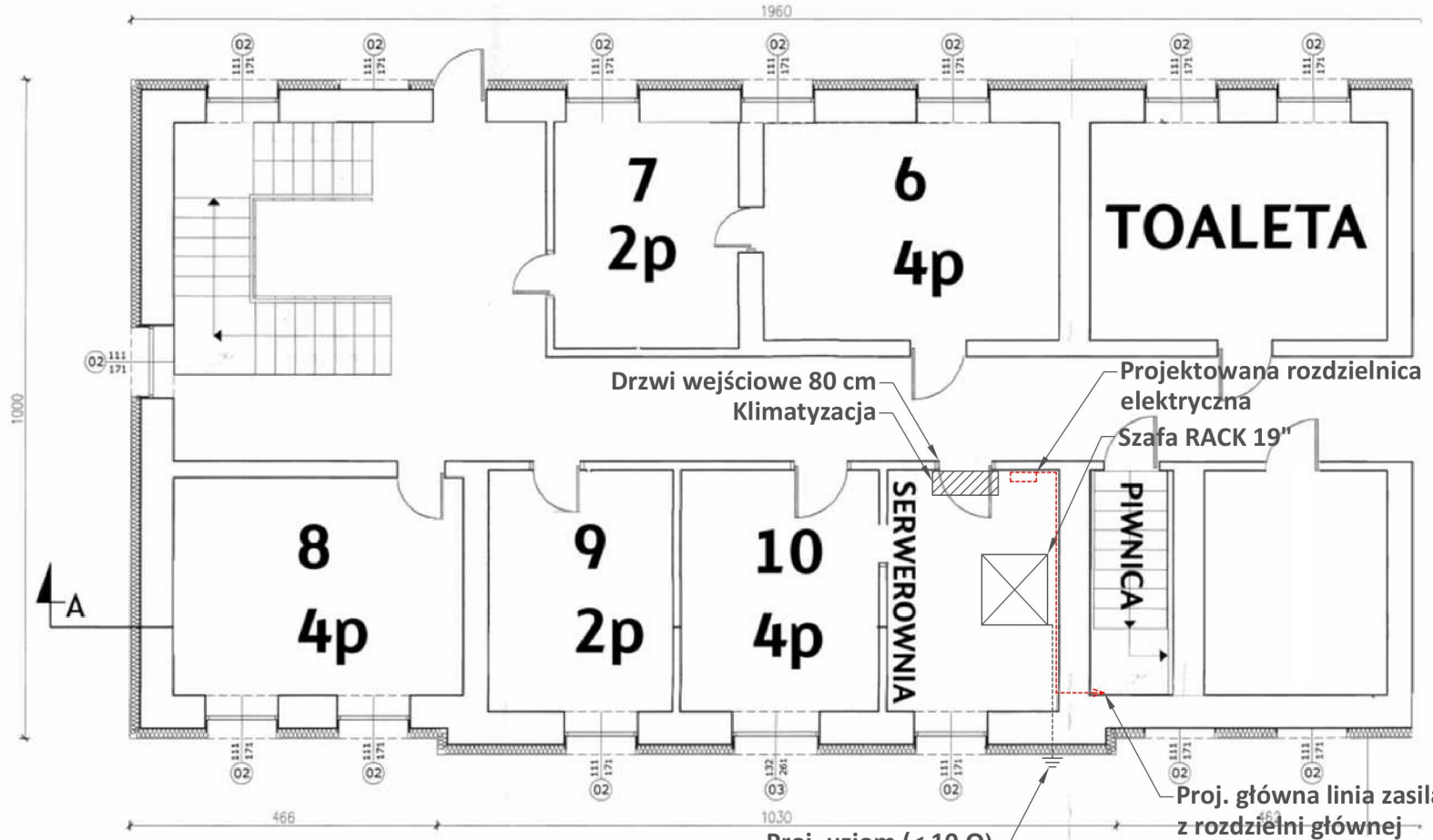
Wykonawca udzieli nie mniej niż 36 miesięczną gwarancję na dostarczane komponenty oraz realizowane prace opisane w niniejszym programie funkcjonalno-użytkowym.

3. Załączniki

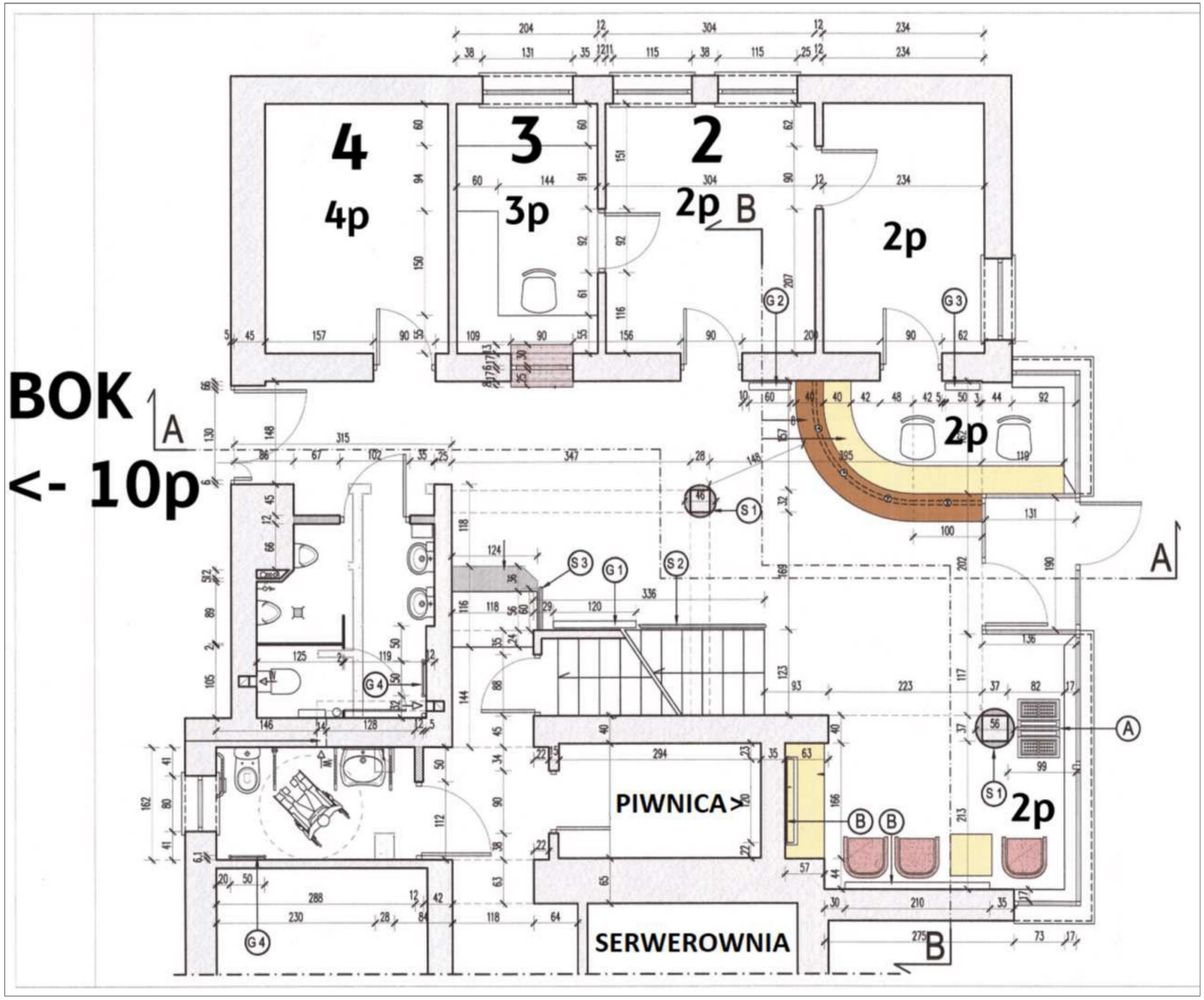
Spis rysunków i załączników:

Lp.	Tytuł dokumentu
1	Rysunek 1 – Plan budynku - Parter
2	Rysunek 2 – Plan budynku parter cz.2
3	Rysunek 3 – Plan budynku – Piętro I
4	Rysunek 4 – Plan budynku – Piętro II
5	Rysunek 4 – Plan budynku – Piętro III

Rysunek 1 – Plan budynku - Parter cz.1



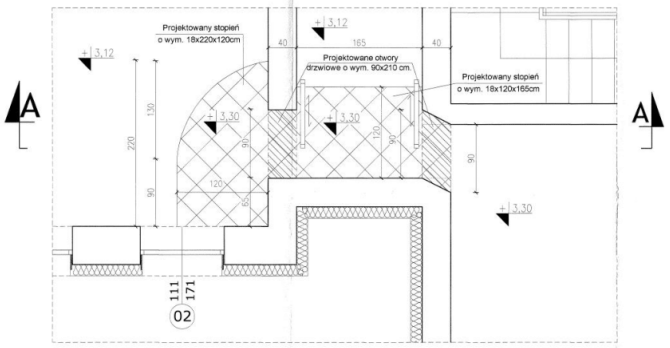
Rysunek 2 – Plan budynku - Parter cz.2



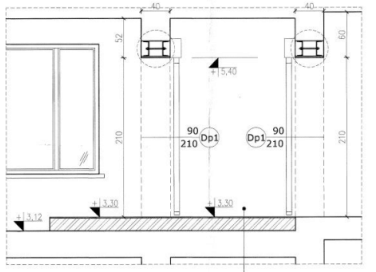
PRZEKRÓJ POZIOMY
SKALA 1:25

Rysunek 3 – Plan budynku – Piętro I

RZUT I PIĘTRA.



PRZEKRÓJ PIONOWY
SKALA 1:25



1cm Terrakota	Stan projektowany
3,5cm Klej Atlas do płytek	
15,0cm Bloczki gazobetonowe	
1,5cm Zaprawa klejowa Atlas	
istniejąca posadzka	Stan istniejący

01 02 - istniejące okna PCV.

D1 D2 D3 D4 - istniejące drzwi wewnętrzne.

Dp3 - Projektowane drzwi wewnętrzne przeszklone o wym. 90x210cm.

Jednostka projektowa:

BIURO PROJEKTOWE
MACIEJ PIERÓG
UL. GŁÓWNA 42, 18-100 ŁAPY
TEL. (086) 716 31 13

Inwestycja:

PROJEKT WYKONAWCZY WYKONANIA ZMIAN OTWORÓW DRZWIOWYCH W ŚCIANACH FONDESZU ISTNIEJĄCYCH POMIESZCZENIAMI NA I PIĘTRZE W BUDYNKU URZĘDU MIEJSKIEGO W ŁAPACH PRZY UL. GEN. W. SIKORSKIEGO 24 NA DZIAŁKACH O NR GEOD. 1035/1 i 3892/1, 18-100 ŁAPY

Inwestor:

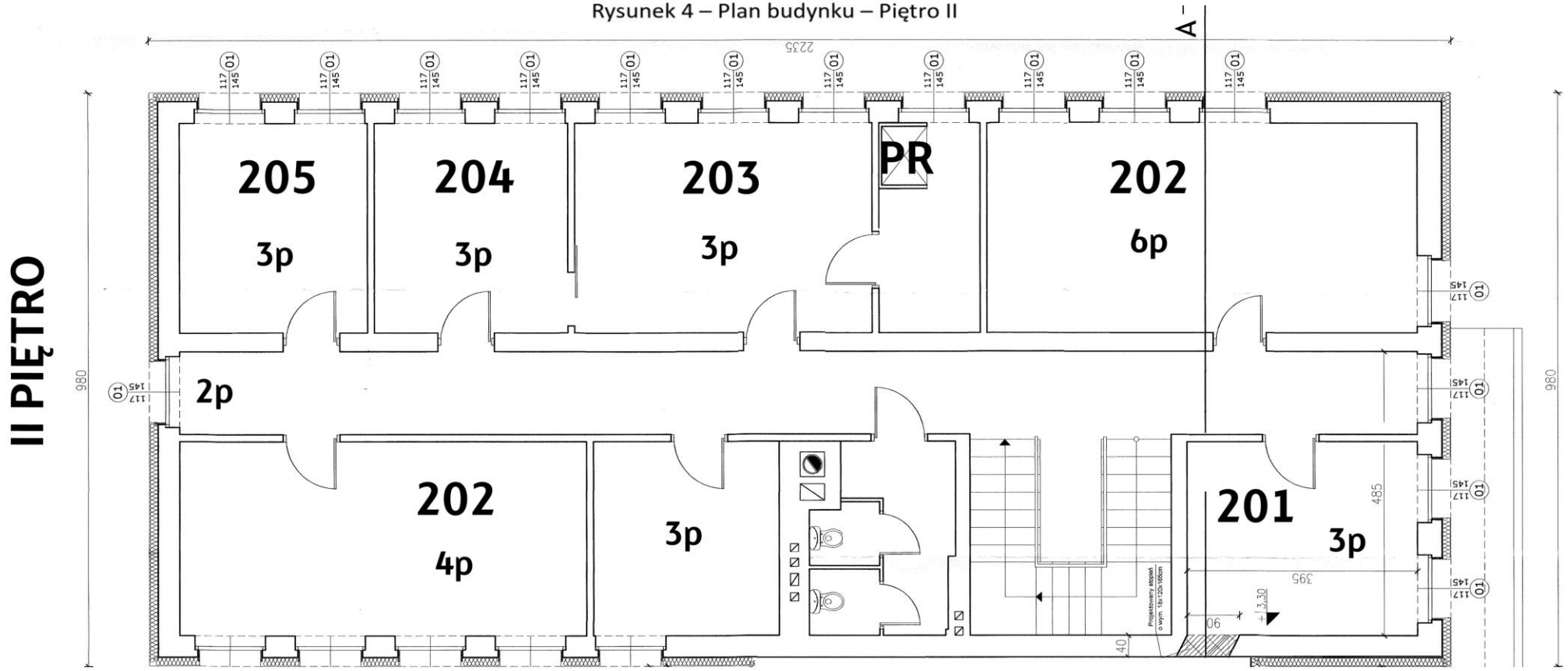
GMINA ŁAPY
UL. GEN. WŁ. SIKORSKIEGO 24
18-100 ŁAPY

Nazwa rysunku:

RZUT I PIĘTRA.

		Nr uprawnień	Podpis
Projektant:	mgr inż. Jerzy Zawadzki	BU/7/0/85 BU/37/289	
Współpraca:	mgr inż. Maciej Pieróg	----------	
Skala: 1:50	Data: 04-01-2010r.	Nr rys. 1	

Rysunek 4 – Plan budynku – Piętro II



Rysunek 5 – Plan budynku – Piętro III