Spis treści

I. Warunki przyłączenia do sieci

II. Opis instalacji teletechnicznej

1. Opis ogólny

Przedmiot opracowania:

Przedmiotem opracowania projektu wykonawczego jest przebudowa budynków istniejących wraz z projektem zagospodarowania oraz projekt łączników między budynkami.

Obiekt:
Budynki przy ul. Ciołka 11A i Astronomów 3 w Warszawie"

Adres budowy:
dz. nr ew. 142/1 i 142/2, ul. Ciołka 11A i Astronomów 3, Warszawa

Inwestor:
Izba Administracji Skarbowej w Warszawie; ul. Alojzego Felińskiego 2B, 01-513 Warszawa

Podstawa opracowania

Niniejsze opracowanie wykonano na podstawie umowy z Inwestorem.

Projekt wykonano na podstawie:
- informacji udzielonych przez użytkownika budynków i Inwestora oraz projektanta na podstawie
- materiałów archiwalnych udostępnionych przez Inwestora
- wizji lokalnej budynku,
- inwentaryzacji budynku opracowanej przez autorów niniejszego opracowania,
- ekspertyzy techniczno-budowlanej
- aktualnych przepisów:

2. Cel i zakres opracowania

Głównym celem opracowania projektu wykonawczego jest uzupełnienie i uszczegółowienie projektu budowlanego w zakresie i stopniu dokładności niezbędnym do sporządzenia przedmiaru robót, kosztorysu inwestorskiego, przygotowania oferty przez wykonawcę i realizacji robót budowlanych.

Zakres opracowania obejmuje w szczególności instalacje:

- System sygnalizacji Pożaru SSP
- Systemy oddymiania grawitacyjnego
- System teleinformatyczny
- System sygnalizacji włamania i napadu
- System kontroli dostępu KD i rejestracji czasu pracy RCP
- System telewizji dozorowej
- System kolejkowy
- System BMS

3. Przepisy i normy

Projekt wykonano zgodnie z niżej wymienionymi normami:

CNBOP wytyczne	Wstęp do automatycznych systemów sygnalizacji pożarowej, oprac. Jerzy Ciszewski, wyd. CNBOP 1996 oraz inne materiały dotyczące projektowania instalacji sygnalizacji pożaru wydawane przez CNBOP w latach 1995-2000.
PKN-CEN/TS 54-14:2006	Specyfikacja Techniczna, Systemy sygnalizacji pożarowej – Część 14: Wytyczne planowania, projektowania, instalowania, odbioru, eksploatacji i konserwacji
PN-EN 50173-1:2013	Informatyka. Instalacje okablowania przeznaczenia ogólnego. Część 1: Wymagania ogólne
PN-EN 50173-2:2008 i PN-EN 50173-2:2008/A1:2011	Informatyka. Instalacje okablowania przeznaczenia ogólnego Część 2: Pomieszczenia biurowe.
PN-EN 50174-1:2010 i PN-EN 50174-1:2010/A1:2011	Technika informatyczna. Instalacja okablowania. Cz.1:Specyfikacja instalacji i zapewnienie jakości
ISO/IEC11801:2002/Am2 :2010	Information technology - Generic cabling for customer premises
PN-EN 50173-5:2009/A2:2013-07	Technika informatyczna. Instalacja okablowania – Część 1- Specyfikacja i zapewnienie jakości
PN-EN 50174-2:2010/A1:2011	Technika informatyczna. Instalacja okablowania – Część 2- Planowanie i wykonawstwo instalacji wewnątrz budynków
PN-EN 50174-3:2014-02	Technika informatyczna. Instalacja okablowania – Część 3 – Planowanie i wykonawstwo instalacji na zewnątrz budynków
PN-EN 50346:2004/A2:2010	Technika informatyczna. Instalacja okablowania - Badanie zainstalowanego okablowania
PN-EN 50288-4-1:2014-02	Przewody wielożyłowe stosowane w cyfrowej i analogowej technice przesyłu danych -- Część 4-1: Wymagania grupowe dotyczące przewodów ekranowanych, testowanych do częstotliwości 600 MHz -- Przewody przeznaczone do poziomego i pionowego układania w budynkach
PN-EN 61935-1:2010E	Wymagania dotyczące sprawdzania symetrycznych i współosiowych kablowych linii

	telekomunikacyjnych -- Część 1: Okablowanie z symetrycznych kabli telekomunikacyjnych zgodne z serią norm EN 50173
PN-ISO/IEC 14763-3:2009/A1:2010P	Technika informatyczna - Implementacja i obsługa okablowania w zabudowaniach użytkowych - Część 3: Testowanie okablowania światłowodowego
PN-EN 60332-1-2:2010/A1:2016-02 PN-EN 60332-3-24:2009 PN-EN 60332-3-22:2009 PN-EN 60754-1:2014-11 PN-EN 60754-2:2014-11 PN-EN 61034-2:2010	Normy międzynarodowe związane z palnością powłoki kabla
PN-EN 50310:2012	Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanym sprzętem informatycznym.
PKN-CLC/TS 50131-7:2011	Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 7: Wytyczne stosowania
PN-EN 50130-4:2012	Systemy alarmowe -- Część 4: Kompatybilność elektromagnetyczna -- Norma dla grupy wyrobów: Wymagania dotyczące odporności urządzeń systemów sygnalizacji pożarowej, sygnalizacji włamania, sygnalizacji napadu, CCTV, kontroli dostępu i osobistych (oryg.)
PN-EN 50130-5:2012	Systemy alarmowe -- Część 5: Próby środowiskowe (oryg.)
PN-EN 50131-1:2009	Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 1: Wymagania systemowe
PN-EN 50131-1:2009/A1:2010	Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 1: Wymagania systemowe
PN-EN 50131-1:2009/IS2:2011	Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 1: Wymagania systemowe
PN-EN 50131-2-2:2009	Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 2-2: Czujki sygnalizacji włamania -- Pasywne czujki podczerwieni
PN-EN 50131-2-3:2010	Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 2-3: Wymagania dotyczące czujek mikrofalowych
PN-EN 50131-2-4:2009	Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 2-4: Wymagania dotyczące dualnych czujek pasywnych podczerwieni i mikrofalowych
PN-EN 50131-2-5:2010	Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 2-5: Wymagania dotyczące dualnych czujek pasywnych podczerwieni i ultradźwiękowych
PN-EN 50131-2-6:2009	Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 2-6: Czujki stykowe (magnetyczne) (oryg.)
PN-EN 50131-3:2010	Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 3: Urządzenia sterujące i obrazujące (oryg.)
PN-EN 50131-4:2010	Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 4: Sygnalizatory (oryg.)

PN-EN 50131-5-3:2011	Systemy alarmowe -- Systemy sygnalizacji włamania -- Część 5-3: Wymagania dotyczące połączeń wzajemnych sprzętu wykorzystującego techniki częstotliwości radiowych
PN-EN 50131-6:2009	Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 6: Zasilanie
PN-EN 50132-1:2010	Systemy alarmowe -- Systemy dozorowe CCTV stosowane w zabezpieczeniach – - Część 1: Wymagania systemowe (oryg.)
PN-EN 50132-5:2002	Systemy alarmowe -- Systemy dozorowe CCTV stosowane w zabezpieczeniach - - Część 5: Teletransmisja (oryg.)
PN-EN 50132-7:2003	Systemy alarmowe -- Systemy dozorowe CCTV stosowane w zabezpieczeniach - - Część 7: Wytyczne stosowania
PN-EN 50133-1:2007	Systemy alarmowe -- Systemy kontroli dostępu w zastosowaniach dotyczących zabezpieczenia -- Część 1: Wymagania systemowe
PN-EN 50133-2-1:2002	Systemy alarmowe -- Systemy kontroli dostępu stosowane w zabezpieczeniach - - Część 2-1: Wymagania dla podzespołów (oryg.)
PN-EN 50133-7:2002	Systemy alarmowe -- Systemy kontroli dostępu stosowane w zabezpieczeniach - - Część 7: Zasady stosowania (oryg.)
PN-EN 50134-1:2007	Systemy alarmowe -- Systemy alarmowe osobiste -- Część 1: Wymagania ogólne Część 2: Urządzenia wyzwalające
PN-EN 50134-3:2002	Systemy alarmowe -- Systemy alarmowe osobiste -- Część 3: Jednostka lokalna i sterownik (oryg.)
PN-EN 50134-5:2005	Systemy alarmowe -- Systemy alarmowe osobiste -- Część 5: Połączenia wewnętrzne i komunikacyjne (oryg.)
PN-EN 50134-7:1999	Systemy alarmowe -- Systemy alarmowe osobiste -- Wytyczne stosowania
PN-EN 50136-1-1:2007	Systemy alarmowe -- Systemy i urządzenia transmisji alarmu -- Część 1-1: Wymagania ogólne dotyczące systemów transmisji alarmu
PN-EN 50136-1-1:2007/A2:2009	Systemy alarmowe -- Systemy i urządzenia transmisji alarmu -- Część 1-1: Wymagania ogólne dotyczące systemów transmisji alarmu
PN-EN 50136-1-2:2007	Systemy alarmowe -- Systemy i urządzenia transmisji alarmu -- Część 1-2: Wymagania dotyczące systemów wykorzystujących łącza dzierżawione
PN-EN 50136-1-3:2007	Systemy alarmowe -- Systemy i urządzenia transmisji alarmu -- Część 1-3: Wymagania dotyczące systemów z komunikatorami cyfrowymi wykorzystujących publiczną komutowaną sieć telefoniczną
PN-EN 50136-1-4:2007	Systemy alarmowe -- Systemy i urządzenia transmisji alarmu -- Część 1-4: Wymagania dotyczące systemów z komunikatorami głosowymi wykorzystujących publiczną komutowaną sieć telefoniczną
PN-EN 50136-1-5:2009	Systemy alarmowe -- Systemy i urządzenia transmisji alarmu -- Część 1-5: Wymagania dotyczące sieci z komutacją pakietów PSN (oryg.)
PN-EN 50136-2-1:2007	Systemy alarmowe -- Systemy i urządzenia transmisji alarmu -- Część 2-1: Wymagania ogólne dotyczące urządzeń transmisji alarmu

PN-EN 50136-2-2:2007	Systemy alarmowe -- Systemy i urządzenia transmisji alarmu -- Część 2-2: Wymagania dotyczące urządzeń stosowanych w systemach wykorzystujących dzierżawione łącza transmisyjne
PN-EN 50136-2-3:2007	Systemy alarmowe -- Systemy i urządzenia transmisji alarmu -- Część 2-3: Wymagania dotyczące urządzeń stosowanych w systemach z komunikatorami cyfrowymi wykorzystujących publiczną komutowaną sieć telefoniczną
PN-EN 50136-2-4:2007	Systemy alarmowe -- Systemy i urządzenia transmisji alarmu -- Część 2-4: Wymagania dotyczące urządzeń stosowanych w systemach z komunikatorami głosowymi wykorzystujących publiczną komutowaną sieć telefoniczną
PN-IEC 839-2-7:1996	Systemy alarmowe -- Włamaniowe systemy alarmowe -- Wymagania i badania pasywnych czujek stłuczenia szyby
PN-E-08390-5:2000	Systemy alarmowe -- Włamaniowe systemy alarmowe -- Wymagania i badania sygnalizatorów
PN-E-08390-22:1993	Systemy alarmowe -- Włamaniowe systemy alarmowe -- Ogólne wymagania i badania czujek
PN-E-08390-23:1993	Systemy alarmowe -- Włamaniowe systemy alarmowe -- Wymagania i badania aktywnych czujek podczerwieni
PN-E-08390-24:1993	Systemy alarmowe -- Włamaniowe systemy alarmowe -- Wymagania i badania ultradźwiękowych czujek Dopplera
BN-84/8984-10.	Zakładowe sieci telekomunikacyjne. Instalacje wewnętrzne. Wymagania ogólne.

4. System sygnalizacji pożaru SSP

4.1 Zakres opracowania

Przewiduje się całkowitą ochronę obu budynków(przy ul. Ciołka oraz Astronowmów) systemem detekcji i sygnalizacji pożaru (SSP). Ochroną objęte zostaną wszystkie pomieszczenia za wyjątkiem pomieszczeń „mokrych".
Dla klatek schodowych przewidziano system sterowania oddymianiem, który przy pomocy central oddymiających będzie otwierał klapy oddymiające na klatkach schodowych. W szybach windowych umieszczone zostały czujki zasysające wyposażone w zestaw rurek zamocowanych do ściany szybu windowego. System SSP będzie również w przypadku zagrożenia w danej strefie otwierał drzwi kontroli dostępu umożliwiając ewakuację oraz dostęp do pomieszczeń z zewnątrz dla służb ratunkowych.

Wszystkie objęte ochroną pomieszczenia i przestrzenie w budynkach będą nadzorowane przez czujki pożarowe oraz w wybranych lokalizacjach ręczne ostrzegacze pożarowe. Ze względu na charakter zagrożenia pożarowego oraz uzyskanie maksymalnie skutecznej ochrony, przewiduje się zastosowanie jako podstawowych czujek dymu i ciepła(lub wielodetektorowych), charakteryzujących się wysoką skutecznością w wykrywaniu pożarów, w których pojawić się może widzialny dym i/lub wzrost temperatury. Czujki te powinny wykrywać pożary testowe od TF1 do TF6 oraz TF8 w zależności od rodzaju pomieszczenia**.** Sensor ciepła powinny reagować na wzrost temperatury występujący podczas pożaru oraz mieć możliwość programowania na działanie zgodnie z klasą A1R lub BR. Wszystkie użyte urządzenia powinny być wyposażone w dwustronne izolatory zwarć.

4.2 Funkcje realizowane przez system SSP:

W przypadku wystąpienia alarmu pożaru w którejkolwiek ze stref budynku realizowana będzie następująca sekwencja działań:

- **Alarm I stopnia**

  a) Alarm pożarowy wstępny, optyczny i akustyczny na centrali SSP,
  b) Uruchomienie drukarki centrali / wizualizacja na PC,

- **Alarm II stopnia**

  a) Pełny alarm pożarowy, alarm optyczny i akustyczny na centrali SSP,
  b) Uruchomienie drukarki centrali / wizualizacja na PC,
  c) Transmisja sygnału alarmu pożarowego do PSP,
  d) Sprowadzenie wind na poziom parteru i pozostawienie otwartych drzwi,
  c) Wyłączenie wentylacji bytowej w całym budynku,
  d) Zamkniecie wszystkich klap na kanałach wentylacji bytowej w całym budynku,
  e) Otwarcie klap na instalacjach oddymiania grawitacyjnego klatki schodowe wraz z załączeniem mechanicznego napowietrzania klatek schodowych,
  f) Otwarcie odpowiednich klap p.poż wentylacji pożarowej w położenie jak do sekwencji pożaru w zależności od strefy pożarowej w której powstał pożar
  g) Wysterowanie centralek oddymiania grawitacyjnego i otwarcie klap oddymiających klatki schodowe, wraz z otwarciem odpowiednich drzwi na parterze,
  h) Załączenie sygnalizatorów optyczno-akustycznych,
  i) Zwolnienie kontroli dostępu na drogach ewakuacji w zależności od miejsca wystąpienia alarmu oraz zawsze na parterze,
  j) Zamknięcie drzwi stale otwartych, jeżeli wystąpią takie sytuacje (oddzielających strefy pożarowe) pożarowych.
  k) Wysterowanie innych instalacji i urządzeń uczestniczących w akcji pożarowej

Sterowane urządzenia należy włączyć do systemu w taki sposób, aby w przypadku uszkodzenia przewodów lub braku napięć zasilających wszystkie sterowane urządzenia znalazły się w pozycji bezpiecznej pożarowo.

W przypadku sterowania elementów ochrony p.poż które wymagają dostarczenia energii elektryczne podczas pożaru, elementy te muszą być zasilane i sterowane przy pomocy kabli o odporności PH 90
System powinien umożliwiać wykonywanie następujących zadań w zakresie monitorowań:

l) monitoring otwarcia/zamknięcia wszystkich klap pożarowych w budynku,
m) monitoring poziomu wody w zbiorniku hydrantowym,
n) monitoring instalacji gaszenia gazem w wybranych pomieszczeniach,

Instalacja sygnalizacji pożarowej została zaprojektowana w oparciu o centralę mikroprocesorową współpracującą z adresowalnymi elementami liniowymi.
Mikroprocesorowy, w pełni automatyczny system sygnalizacji pożaru powinien umożliwiać osiągnięcie bardzo wysokiej czułości i niezawodnej pracy instalacji. Centrala SSP powinna posiadać następujące cechy funkcjonalne:

- redundantny układ mikroprocesorowy wraz z pamięcią,
- pracować w systemie adresowalnym tzn. umożliwiać identyfikację numeru i rodzaju elementu zainstalowanego w pętli dozorowej,
- mieć wbudowaną pamięć zdarzeń i alarmów,
- mieć duży, czytelny, dotykowy wyświetlacz LCD umożliwiający uzyskanie pełnej informacji, dotyczącej stanu systemu oraz ułatwiający konfiguracją i obsługę centrali,
- mieć wbudowaną drukarkę umożliwiającą wydruk pamięci zdarzeń,
- umożliwić podłączenie adresowalnych elementów liniowych, służących do sterowania i kontroli urządzeń dodatkowych, współpracujących z systemem p.poż,
- umożliwić podłączenie adresowalnych elementów liniowych z odgałęzieniami bocznymi dla czujek konwencjonalnych,
- umożliwić blokowanie alarmów pochodzących od elementów liniowych na określony czas lub na stałe,
- współpracować z urządzeniami monitoringu pożarowego,
- posiadać modułową architekturę, by dobrze dostosować możliwości centrali do potrzeb obiektu,
- umożliwić sterowanie urządzeniami przeciwpożarowymi za pomocą wyjść przekaźnikowych fail-safe,
- umożliwić kontrolowanie stanu urządzeń przeciwpożarowych z użyciem wejść kontrolnych trójstanowych,
- umożliwić pracę w trybie rozproszonym, w którym centrala komunikuje się z węzłami, posiadającymi moduły funkcjonalne, z lub bez dodatkowych paneli operatorskich, co umożliwi obniżenie kosztów instalacji i zwiększy elastyczność systemu,
- umożliwić grupowanie sterowań urządzeniami przeciwpożarowymi,
- umożliwić synchroniczne wysterowanie do kilkudziesięciu wyjść sterujących jednocześnie,
- umożliwić synchroniczne wysterowanie do kilkudziesięciu adresowalnych sygnalizatorów tonowych lub głosowych,
- umożliwić przeprowadzenie konfiguracji za pomocą klawiatury i myszki komputerowej łączących się z centralą przez port USB,
- umożliwiać przesłanie konfiguracji do centrali z pamięci flash typu pendrive,
- umożliwić podłączenie do 250 elementów adresowalnych na jednej linii dozorowej,
- umożliwić podłączenie do 398 linii dozorowych typu A lub B,
- umożliwić wykonanie testowania lub blokowania elementów oraz przygotowanie odpowiedniego raportu,
- umożliwić podłączenia systemu komputerowego w celu przedstawienia stanu systemu w formie graficznej na ekranie monitora,
- umożliwić wysterowanie i zasilanie sygnalizatorów alarmowych konwencjonalnych,
- umożliwić podłączenie centrali sterującej oddymianiem bezpośrednio przez linię dozorową, jako element adresowalny, dając możliwość kontrolowania stanu urządzeń przeciwpożarowych oraz wysterowania tych urządzeń na sygnały z CSP,
- możliwość weryfikacji, czy elementy pętlowe znajdują się w przeznaczonych dla nich miejscach oraz czy nie została zamieniona ich kolejność zainstalowania,
- umożliwiać podłączenie czujek liniowych dymu bezpośrednio na liniach dozorowych centrali.

4.3 Organizacja alarmowania:

W obiekcie przyjmuje się organizację ogólną dwustopniową alarmowania.
Dla pomieszczeń, w których mogą występować czynniki powodujące fałszywe alarmy (np. duże zapylenie lub zakłócenia elektromagnetyczne) przewidziano możliwość połączenia czujek w jedną strefę dozorową i ustawienie odpowiedniego wariantu alarmowania np. koincydencji lub wstępnego kasowania, eliminującego ewentualne mylne zadziałania czujek.

Zakłada się całodobową obsługę obiektu.
Czasy opóźnień T1, T2, T3 należy uzgodnić z Inwestorem i ustawić tak, aby były możliwie najkrótsze. Proponuje się ustawienie czasów:
T1 = 30 s na pierwsze potwierdzenie alarmu przez obsługę centrali,
T2 = 3 min czas na sprawdzenie przez obsługę zdarzenia pożarowego,
T3 = 3 min 30 s czas opóźnień uruchomienia pożarowych urządzeń alarmowych .

UWAGA! Na etapie wykonawstwa, w obszarach chronionych przez system sygnalizacji pożaru, w przypadku wystąpienia jakichkolwiek dodatkowych przestrzeni lub stref nieujętych w niniejszej dokumentacji należy uzgodnić z projektantem i następnie zabezpieczyć je bezwzględnie odpowiednimi detektorami.

4.4 Założenia do scenariusza pożarowego:

Centrala sygnalizacji pożarowej powinna sygnalizować alarm I stopnia w przypadku zadziałania jednej z czujek pożarowych.

ALARM I STOPNIA:

- **Przeszkolony personel** (obsługa) powinna zidentyfikować (odczytać) miejsce wystąpienia alarmu, wyciszyć sygnalizację wewnętrzną w centrali, zawiesić ogłoszenie alarmu o czas na zweryfikowanie zagrożenia pożarowego (prawdziwe lub fałszywe) np. na 180 sekund. W przypadku zweryfikowania alarmu jako fałszywy, alarm w centrali należy skasować, w przypadku potwierdzenia prawdziwości alarmu należy bezzwłocznie zainicjować alarm II przez wciśnięcie przycisku ROP.

ALARM II STOPNIA:

Centrala powinna sygnalizować alarm II stopnia w przypadku:
- przekroczenia kryterium czasowego podanego powyżej,
- wciśnięcia przez użytkownika przycisku ROP,
- zadziałania dwóch lub więcej detektorów,
- przyjęcia alarmu pożarowego z urządzeń kontrolno-sterujących.

Dwa ostatnie punkty dotyczą przypadku z odpowiednio ustawionym wariantem alarmowania w strefie.

4.5 Lokalizacja centrali:

Montaż centrali master przewidziano w pomieszczeniu CENTRAL DOZORU na poziomie -1 w budynku przy ul. Ciołka. Bezpieczeństwo centrali zapewnia objęcie pomieszczenia ochroną czujkami dymu i przyciskiem ROP. Dodatkowa centrala (Slave) została zlokalizowana w budynku przy ul. asntronomów w pom. Teletechnicznym na poziomie -1 i będzie połaczona sieciowo z centralką główną (master).

W miejscu obsługi systemu należy umieścić skróconą instrukcję obsługi centrali.

W projektowanej instalacji sygnalizacji pożarowej przewiduje się zastosowanie linii dozorowych typu A centrali, na których zainstalowane będą adresowalne czujki, ręczne ostrzegacze pożarowe, oraz linii na których zainstalowane będą liniowe moduły kontrolno-sterujące przeznaczone do uruchamiania, sterowania urządzeniami alarmowymi i przeciwpożarowymi oraz do monitorowania urządzeń związanych z bezpieczeństwem pożarowym obiektu

Projektowana instalacja SSP opierać się będzie na urządzeniach:
- Wielosensorowych oraz czujkach dymu
- adresowalnych, ręcznych ostrzegaczach pożarowych,
- adresowalnych modułach wejść / wyjść,
- wskaźnikach zadziałania.

Urządzenia te powinny posiadać aktualne certyfikaty i świadectwa dopuszczenia (dla urządzeń, które tego wymagają) pozwalające na ich stosowanie w ochronie przeciwpożarowej na terenie RP.

4.6 Zasilanie systemu

Centrale należy zasilić z wydzielonego obwodu elektrycznego sprzed głównego wyłącznika przeciwpożarowego prądu, do którego nie należy podłączać żadnych innych urządzeń. Na wypadek awarii zasilania głównego system zostanie wyposażony w zasilanie rezerwowe w postaci akumulatorów. Pojemność baterii akumulatorów zasilania rezerwowego CSP powinna umożliwić utrzymanie instalacji w stanie pracy przez co najmniej 72 h, po czym pojemność ta musi być wystarczająca do zapewnienia alarmowania jeszcze co najmniej przez 30 min.
Jeżeli uszkodzenie będzie natychmiast zgłaszane służbie serwisowej przez nadzór nad instalacją, a w zawartej umowie o konserwację zapewnia się dokonanie naprawy w czasie krótszym niż 24 h, minimalna pojemność baterii akumulatorów zasilania rezerwowego może być zmniejszona do wartości odpowiadającej zmniejszeniu czasu dozorowania z 72 h do 30 h. czas ten można dalej skrócić aż do 4 h, jeżeli przez całą dobę na miejscu są do dyspozycji części zamienne, służby serwisowe i awaryjny zespół prądotwórczy lub zapasowa bateria rezerwowa.
Po obliczeniu minimalnej pojemności baterii zasilania rezerwowego należy sprawdzić, czy urządzenie ładujące gwarantuje ponowne naładowanie baterii rozładowanej do jej końcowego napięcia rozładowania do co najmniej 80% jej pojemności znamionowej w ciągu 24 godzin, zaś do jej pojemności znamionowej w ciągu następnych 48 godzin.
Do akumulatorów nie można przyłączyć innych odbiorników energii, niebędących elementem sytemu sygnalizacji pożaru.

4.7 Okablowanie systemu

Linie dozorowe należy wykonać telekomunikacyjnym kablem stacyjnym o izolacji PVC i uniepalnionej powłoce PVC w kolorze czerwonym, ekranowanym, do zastosowań w systemach przeciwpożarowych typu YnTKSYekw 1x2x0,8. Linie dozorowe na których zainstalowane są moduły kontrolno-sterujące przeznaczone do uruchamiania, sterowania urządzeniami alarmowymi i przeciwpożarowymi oraz do monitorowania urządzeń związanych z bezpieczeństwem pożarowym obiektu należy wykonać telekomunikacyjnym kablem stacyjnym do instalacji przeciwpożarowych koloru czerwonego typu HTKSHekw 1x2x0,8 o klasie odporności ogniowej PH90.

Linie sterowania klap p.poż. w instalacjach oddymiania oraz linie zasilające sygnalizatory optyczno-akustyczne należy wykonać np. ognioodpornym, bezhalogenowym kablem elektroenergetycznym koloru czerwonego typu HDGs 3x1,5 lub o innej średnicy z zachowaniem odpowiednich parametrów.
Linie monitorowania klap p.poż. w instalacjach oddymiania należy wykonać telekomunikacyjnym kablem stacyjnym do instalacji przeciwpożarowych koloru czerwonego typu HTKSHekw 1x2x0,8 o klasie odporności ogniowej PH90.

Linie sterowania elementami automatyki budynkowej (wentylacja, windy, drzwi) należy wykonać np. telekomunikacyjnym kablem stacyjnym do instalacji przeciwpożarowych kolory czerwonego typu HTKSHekw 1x2x1,0 o klasie odporności ogniowej PH90. Kable powinny posiadać aktualne certyfikaty.

4.8 Montaż urządzeń i instalacji

Montaż urządzeń i wyposażenia powinien zostać wykonany zgodnie z dokumentacją techniczno-ruchową urządzeń przez wykwalifikowanego instalatora.
Przy montażu urządzeń należy przestrzegać następujących zasad:

- czujki wraz z gniazdami należy instalować na sufitach w miejscach oznaczonych w dokumentacji,
- odległość instalowania czujek nie powinna być mniejszej niż 0,5 m od ścian, przewodów energetycznych, żarowych opraw oświetleniowych,
- czujki powinny być instalowane w taki sposób aby widoczna była dioda LED sygnalizująca zadziałanie,
- w pomieszczeniach, gdzie występują podciągi, belki lub przebiegają pod stropem kanały wentylacyjne, w odległości nie mniejszej niż 25 cm od stropu, odległość instalowania czujek od tych elementów nie powinna być mniejsza niż 0,5 m,
- odległość instalowanie nie powinna być mniejsza niż 1,5 m od otworów wlotowych i wylotowych wentylacji oraz klimatyzacji,
- sufity perforowane, przez które jest doprowadzane powietrze do pomieszczenia powinny być zakryte w promieniu min. 0,6 m wokół czujki,
- czujek nie należy instalować w atmosferze korozyjnej, zawierającej gazy i opary żrące oraz zapylenie,
- dodatkowe wskaźniki zadziałania powinny być instalowane w najbliższej możliwej odległości od czujki, w miejscach gdzie będą dobrze widoczne,
- w uzasadnionych przypadkach istnieje możliwość przesunięcia punktowej czujki w stosunku do położenia

przedstawionego na planie. Należy jednak wówczas przyjąć ogólną zasadę, by odległość pozioma od czujki do najdalszego dozorowanego punktu tego pomieszczenia nie była większa niż maksymalne zasięgi czujek czyli 7,5 m dla czujek dymu, 5 m dla czujek ciepła,

- dopuszcza się zmianę kolejności łączenia czujek w ramach jednej linii dozorowej, wszystkie zmiany należy umieścić w dokumentacji powykonawczej,
- ręczne ostrzegacze pożarowe należy instalować na ścianach, na wysokości od 1,2 m do 1,6 m od poziomu podłogi w taki sposób, aby były dobrze widoczne i dostępne,
- przewody instalacji SSP należy układać w odległości minimum 0,3 m od kabli innych instalacji, w szczególności zasilających i biegnących równolegle. Przecięcia zespołów kablowych, których nie można uniknąć, wykonać pod kątem 90 stopni,
- łączenie przewodów należy wykonywać tylko w gniazdach czujek lub na zaciskach modułów; należy unikać dodatkowych połączeń w puszkach instalacyjnych. Przejścia przez ściany winny być wykonane w rurkach instalacyjnych,
- ekran przewodów musi być połączony między sobą w poszczególnych punktach montażowych (np. w gniazdach, w specjalnym złączu). Przed instalacją czujek pożarowych należy sprawdzić ciągłość żył i ekranu oraz oporność i pojemność kabli linii dozorowej, które nie mogą przekroczyć wartości właściwych dla systemu,
- przewody instalacji sygnalizacji pożaru należy prowadzić w bruzdach wykutych w ścianach, sufitach lub w specjalnych trasach kablowych zgodnie z obowiązującymi przepisami,
- przed montażem zweryfikować i potwierdzić u Inwestora szczegółowe rozplanowanie tras kablowych innych instalacji,
- wszystkie przejścia kablowe między strefami pożarowymi uszczelnić zgodnie z obowiązującymi przepisami, materiałami o odpowiedniej odporności ogniowej, zgodnej z wymaganą klasą PH.

4.9 Elementy wchodzące w skład systemu

A. Centrala sygnalizacji pożarowej przeznaczona do stosowania:
   - szczególnie w obiektach o skomplikowanej budowie lub rozproszonych na rozległym terenie, z dużą liczbą współpracujących urządzeń automatyki pożarowej,
   - doskonale nadaje się do stosowania w odpowiedzialnych instalacjach bezpieczeństwa „inteligentnych" budynków ze względu na zdolność do przekazywania dużej ilości informacji cyfrowych do systemów integracji i nadzoru.

Uniwersalna centrala sterująca przeznaczona do uruchamiania urządzeń przeciwpożarowych, służących do oddymiania grawitacyjnego i mechanicznego.

B. Czujki:
   - adresowalna wielostanowa, wielosensorowa czujka optyczno-termiczna
   - czujka zasysająca dymu
C. Ręczne ostrzegacze pożarowe: ręczny ostrzegacz pożarowy do zastosowań wewnątrz budynków
D. Elementy wejść/wyjść:
   - element kontrolno-sterujący 2 wej – 2 wyj
   - element kontrolno-sterujący 4 wej
   - element kontrolno-sterujący 4 wyj
   - element kontrolno-sterujący 4 wej – 4 wyj
E. Przyciski:
   - ręczne przyciski oddymiania
   - przyciski przewietrzania

4.10 Opis dobranych urządzeń

Centrale pożarowe:

- centrala sygnalizacji pożarowej, przeznaczona do :
- wykrywania i sygnalizowania zagrożenia pożarowego po odebraniu informacji od współpracujących z nią czujek i ręcznych ostrzegaczy pożarowych,
- koordynowania pracy wszystkich urządzeń w systemie oraz podejmowania decyzji o zainicjowaniu alarmu

pożarowego,
- wysterowaniu urządzeń sygnalizacyjnych i przeciwpożarowych oraz o przekazaniu informacji do centrum monitorowania lub systemu nadzoru,
- ochrony przeciwpożarowej różnego rodzaju obiektów, zwłaszcza dużych lub rozległych np. hoteli, biurowców, magazynów, obiektów zabytkowych, „inteligentnych" budynków z dużą liczbą współpracujących urządzeń automatyki pożarowej.

Została zaprojektowana na bazie koncepcji urządzenia modułowego o architekturze rozproszonej. Składa się z wielu zunifikowanych modułów różnych typów, umieszczonych w standardowych obudowach, które pojedynczo lub połączone w zestawy (tzw. węzły), mogą być rozmieszczone w różnych punktach chronionego obiektu, nawet znacznie od siebie oddalonych. Odległości pomiędzy węzłami centrali mogą wynosić do 1200 m w przypadku kabla miedzianego lub nawet do 15 kilometrów w przypadku stosowania światłowodu jednomodowego. Wszystkie moduły, w obrębie pojedynczego węzła oraz węzły pomiędzy sobą, połączone są wspólną, podwójną (redundantną) cyfrową magistralą komunikacyjną.

Centrala SSP składa się z:
- paneli sterujących z wyświetlaczem,
- modułów funkcjonalnych:
  - linii dozorowych,
  - kontrolno-sterujących,
  - wyjść przekaźnikowych,
  - wyjść potencjałowych,
  - wyjść przekaźnikowych wysokonapięciowych,
  - wejść kontrolnych,
  - zasilania,
  - drukarek,
  - transmisji,

Panele sterujące oraz moduły, zamontowane są w obudowach o standardowych wymiarach, które można ze sobą łączyć mechanicznie. Połączone mechanicznie obudowy tworzą węzeł centrali. Każdy węzeł musi być wyposażony w przynajmniej jeden moduł zasilacza. Centrala musi posiadać przynajmniej jeden węzeł, w którym zamontowany jest główny panel. Jest to tzw. węzeł główny centrali i może być tylko jeden w instalacji. Pozostałe wyposażenie centrali tworzy tzw. węzły wyniesione, które muszą być podłączone do węzła głównego centrali. Komunikacja pomiędzy węzłami odbywa się za pomocą zdublowanego połączenia kablowego (RS-485) lub zdublowanej pary światłowodów. W każdym węźle centrali (oprócz zasilacza) mogą znajdować się moduły funkcjonalne realizujące podłączenie linii dozorowych, lub do bezpośredniego sterowania lub kontroli urządzeń automatyki pożarowej. W każdym węźle wyniesionym może znajdować się panel sterujący pełniący funkcję dodatkowego terminala obsługowego oraz redundantnego kontrolera w przypadku awarii węzła Master.

Charakterystyka ogólna systemu:

System sygnalizacji pożarowej tworzy nowa centrala o architekturze rozproszonej i szereg elementów liniowych (czujek pożarowych, elementów kontrolno-sterujących, sygnalizatorów akustycznych).
System SSP może chronić średnie, duże i bardzo duże obiekty. Szczególnie obiekty o skomplikowanej budowie lub rozproszone na rozległym terenie, z dużą liczbą współpracujących urządzeń automatyki pożarowej (czyli ze złożonymi scenariuszami zdarzeń). Doskonale nadaje się do stosowania w odpowiedzialnych instalacjach bezpieczeństwa "inteligentnych" budynków ze względu na zdolność do przekazywania dużej ilości informacji cyfrowych do systemów integracji i nadzoru. Stąd może być łatwo integrowany w ramach wielu istniejących na rynku systemów zarządzania bezpieczeństwem obiektu.

- Uniwersalna centrala sterująca, przeznaczona do:

Uruchamiania urządzeń przeciwpożarowych, służących do oddymiania grawitacyjnego i mechanicznego (klapy przeciwpożarowe oddymiające i odcinające), oraz dziennego przewietrzania.

Przystosowana jest do pracy ciągłej w pomieszczeniach o małym zapyleniu, w zakresie temperatur od - 10 °C do + 55 °C i przy wilgotności względnej powietrza do 80 % przy + 55 °C.
Umożliwia:

- wykrywanie pożaru (zadymienia),
- uruchamianie automatyczne lub ręczne urządzeń przeciwpożarowych, instalowanych w systemach oddymiania,
- sygnalizowanie akustyczne i optyczne stanów pracy urządzeń (alarm, uszkodzenie),
- automatyczną kontrolę zadziałania urządzeń przeciwpożarowych i wykonawczych (siłowniki, elektromagnesy, wentylatory itp.) systemu oddymiania,
- automatyczną kontrolę własnych układów i obwodów centrali,
- przekazywanie podstawowych informacji do systemów nadrzędnych o alarmie, uszkodzeniu, stanie urządzeń przeciwpożarowych i wykonawczych,

Może pracować indywidualnie jako jedno lub wielostrefowy uniwersalny sterownik oddymiania lub w adresowalnych liniach / pętlach dozorowych central sygnalizacji pożarowej. W ramach pracy na adresowalnej linii dozorowej centrala posiada obustronne izolatory zwarć. Ze względu na różnorodność zasilania i sterowania siłowników i napędów elektrycznych urządzeń przeciwpożarowych przewidziano sterowanie siłowników dwukierunkowych, dwuprzewodowych lub trzyprzewodowych, siłowników ze sprężyną powrotną, trzymaczy drzwiowych oraz elektrozaczepów. Centrala współpracuje z ręcznymi przyciskami oddymiania oraz przyciskami przewietrzania.
Posiada możliwość współpracy z automatyką pogodową różnych producentów. Modułowa budowa centrali pozwala na wykorzystanie szeregu uniwersalnych wejść i wyjść do podłączenia zewnętrznych instalacji systemu oddymiania. Centrala posiada wewnętrzną pamięć zdarzeń, może zarejestrować do 1000 wpisów. Konfigurowana przez port USB.

Czujki:

- wielosensorowa czujka dymu i ciepła, przeznaczona do wykrywania początkowego stadium rozwoju pożaru, podczas którego pojawia się dym i/lub następuje wzrost temperatury. Charakteryzuje się znaczną odpornością na ruch powietrza i na zmiany ciśnienia. Może pracować w adresowalnych pętlowych liniach dozorowych central sygnalizacji pożarowej.
  Czujka wyposażona jest w wewnętrzny izolator zwarć. Instalowana jest w gnieździe. Wykrywa pożary testowe od TF1 do TF6 oraz TF8. Czujka ma możliwość czyszczenia lub wymiany labiryntu.
- Zasysająca czujka dymu charakteryzująca się wysoką czułością dzięki dyspersji światła laserowego umożliwiającą ultrawczesne wykrywanie dymu. Maksymalna długość rurek ssących- do 50 m + 60m rurek kapilarowych.
  Dynamiczna nastawa parametrów detektora w zależności od pory dnia i zadymienia otoczenia. Inteligentna kompensacja czułości przy zmieniającym się poziomie zadymienia tła w układach dziennych, tygodniowych, miesięcznych i rocznych. Automatycznie ustawia właściwą czułość pod względem warunków panujących w obszarze chronionym (transformatornie, magazyny, szyby windowe itp.).
  Automatyczne lub ręczne tłumienie czułości o zadany procent dla eliminacji zjawisk powodujących fałszywe alarmy jak: palacze, wyziewy przemysłowe, wózki spalinowe, odkurzacze przemysłowe.

Ręczne ostrzegacze pożarowe:

- ręczny ostrzegacz pożarowy jest przeznaczony do pracy w adresowalnych pętlach dozorowych central sygnalizacji pożarowej. Jest przeznaczony do przekazywania informacji o zauważonym pożarze poprzez ręczne uruchomienie. Ostrzegacze wyposażone są w wewnętrzne izolatory zwarć, przewidziany jest do instalowania wewnątrz obiektów, temperatura pracy -25°C do +55°C i wilgotności względnej do 95 % przy 40°C, szczelność obudowy IP 30.

Elementy wejść/wyjść:

- uniwersalny element kontrolno-sterujący przeznaczony do :
  - sterowania automatycznych urządzeń zabezpieczających, przeciwpożarowych,
  - kontroli zadziałania ww. urządzeń,
  - sterowania sygnalizatorami,
  - kontroli stanu dowolnych urządzeń.

Wejścia niskonapięciowe (NN) elementu umożliwiają podłączenie niezależnych, bez-potencjałowych zestyków normalnie zwartych lub normalnie rozwartych. Wejścia wysokonapięciowe (WN) elementu umożliwiają podłączenie niezależnych zestyków przy napięciu do 230 VAC lub 220 VDC. Przystosowany jest do pracy wewnątrz i na zewnątrz obiektów (szczelność obudowy IP66) w zakresie temperatur od -40°C do +85°C i wilgotności względnej do 95 % przy

40°C. Przewidziany jest do pracy wyłącznie w adresowalnych liniach dozorowych central sygnalizacji pożarowej. Dostępne są np. w klku odmianach konfiguracyjnych oznaczonych jako:

- wyposażony w 4 wejścia niskonapięciowe,
- wyposażony w 4 wyjścia,
- wyposażony w 2 wejścia niskonapięciowe, 2 wyjścia,
- wyposażony w 4 wejścia niskonapięciowe, 4 wyjścia,
- wyposażony w 2 wejścia wysokonapięciowe, 2 wyjścia,
- wyposażony w 4 wejścia wysokonapięciowe.

Element kontrolno-sterujący wyposażony jest w wewnętrzny izolator zwarć, który odcina sprawną część linii dozorowej od sąsiadującej części zwartej. Max. prąd przełączny dla styków przekaźnika to 2 A, max napięcie 250 VAC / 220 VDC, max. moc 62,5 VA / 60 W. Działanie elementów może być programowane i polega na wyborze:

- rodzaju pracy wyjścia sterującego,
- możliwości kontroli ciągłości przewodu podłączonego do wyjścia sterującego,
- stany bezpiecznego wyjścia sterującego – funkcja „fail safe”,
- funkcji jaką spełnia wejście,
- sposobu działania wejścia niskonapięciowego (NO, NC) lub wejścia wysokonapięciowego,
- czasów opóźnienia wysterowania, wysterowania, opóźnienia kasowania i kasowania.

Przyciski:

- ręczny przycisk oddymiania, przeznaczony jest do współpracy z uniwersalną centralą UCS, służy do uruchomienia oraz kasowania klap oddymiających poprzez centralę. Wyposażony jest w trzy diody sygnalizacyjne (URUCHOMIENIE, OK – DOZÓR, USZKODZENIE). Przeznaczony jest do montażu natynkowego i wtynkowego w instalacjach wewnątrz obiektów. Temperatura pracy od -25°C do +55°C i wilgotności względnej do 95 % przy 40°C. Łączenie z centralą przy pomocy 6 żyłowego przewodu.

4.11 System oddymiania grawitacyjnego

W obu budynkach przewiduje się zastosowanie instalacji oddymiania grawitacyjnego na klatkach schodowych.

Otwarcie okna oddymiającego może nastąpić poprzez:

- wykrycie dymu przez czujki pożarowe systemu SSP zainstalowane w klatkach schodowych/szybach/salach operacyjnych i automatyczny sygnał z systemu SSP do centralki
- wciśnięcie ręcznego przycisku oddymiania,
- wciśniecie przycisku przewietrzania, funkcja pomocnicza dla utrzymania komfortu

Dodatkowo w celu prawidłowej sprawności działania wentylacji grawitacyjnej wraz z uruchomieniem otwarcia okna oddymiającego automatycznie zostaną otwarte wybrane drzwi służące doprowadzeniu świeżego powietrza.
Każdy system będzie składał się z następujących elementów:

- centralki oddymiania z baterią akumulatorów zainstalowanej na ostatniej kondygnacji np: w klatce schodowej, szachtach tlt,
- centralek sterowania drzwiami zainstalowanymi na kondygnacji parteru,
- ręcznych przycisków oddymiania zainstalowanych w klatce schodowej na ostatniej kondygnacji, kondygnacjach pośrednich oraz w pomieszczeniu ochrony na parterze,
- przycisków przewietrzania w klatce schodowej na ostatnich kondygnacjach i na parterze w pom. ochrony,
- czujek dymu budynkowego systemu SSP,

Centralki oddymiania i sterowania drzwiami zostaną połączone z budynkowym systemem SSP w celu sterowania i monitoringu zadziałania lub awarii systemu.

4.12 Odbiór prac

Przed przekazaniem systemu do eksploatacji Wykonawca powinien przekazać:

- dokumentację powykonawczą zawierającą zaktualizowany projekt techniczny z naniesionymi i uzgodnionymi zmianami powstałymi w czasie wykonawstwa,
- ważne świadectwa dopuszczenia wydane przez CNBOP w Józefowie na zastosowane urządzenia lub certyfikaty,

- protokoły z pomiarów.

oraz dokonać próbnego uruchomienia systemu.
Uruchamiający powinien sprawdzić czy:

- sposób wykonania instalacji jest zadawalający,
- metody, materiały i elementy zostały użyte zgodnie z obowiązującymi przepisami,
- dokumentacja powykonawcza (rysunki i opisy) są zgodne z instalacją,
- wszystkie czujki i ręczne ostrzegacze pożarowe są sprawne,
- informacje przekazywane przez CSP są prawidłowe i spełniają wymagania zawarte w dokumentacji,
- wszystkie połączenia do stacji odbiorczej sygnałów lub PSP są prawidłowe,
- wszystkie urządzenia alarmowe działają zgodnie z zaleceniami zawartymi w projekcie.

4.13 Zalecenia dla Użytkownika

W pomieszczeniu ochrony lub innym gdzie została zainstalowana centrala sygnalizacji pożarowej należy umieścić:

- instrukcję obsługi centrali,
- instrukcję postepowania w przypadku wystąpienia alarmu pożarowego lub uszkodzenia,
- plan sytuacyjny z zaznaczeniem dojść do pomieszczeń,
- książkę przeglądów okresowych,
- wykaz osób powiadamianych.

Użytkownik powinien dopilnować, aby Wykonawca przeprowadził odpowiednie szkolenie osób zajmujących się systemem SSP.
Po przekazaniu systemu do eksploatacji należy zlecić stałą konserwację urządzeń i instalacji, wymóg taki jest zapisany w specyfikacji technicznej PKN-CEN/TS 54-14:2006.

4.14 Konserwacja systemu

Na podstawie specyfikacji technicznej PKN-CEN/TS 54-14 poniżej przedstawiono warunki eksploatacji systemu SSP. Wymagania te określają ramowy i szczegółowy zakres prac konserwacyjnych oraz obsługi technicznej.

Obsługa codzienna:

Użytkownik lub właściciel powinien zapewnić, aby codziennie było sprawdzane:

- czy każda centrala, tablica i panel wskazują stan dozorowania lub, czy każde odchylenie od stanu dozorowania jest odnotowane w książce pracy i, czy we właściwy sposób została zawiadomiona firma prowadząca konserwację,
- czy przy każdym alarmie zarejestrowanym od poprzedniego dnia podjęto odpowiednie działania,
- czy jeśli instalacja była wyłączona, sprawdzana lub wyciszana, to to została przywrócona do stanu dozorowania.

Każda zauważona nieprawidłowość powinna być odnotowana w książce pracy i możliwie szybko usunięta.

Obsługa miesięczna:

Co najmniej raz w miesiącu użytkownik lub właściciel powinien zapewnić aby:

- zapasy papieru, tuszu lub taśmy dla każdej drukarki były wystarczające,
- przeprowadzono próby rozruchu każdego awaryjnego zespołu prądotwórczego, który powinien spełniać oraz sprawdzono zapas paliwa – i w razie potrzeby – uzupełniono,
- przeprowadzono test wskaźników a każdy fakt niesprawności wskaźnika został odnotowany.

Każda zauważona nieprawidłowość powinna być odnotowana w książce pracy i możliwie szybko usunięta.

Obsługa kwartalna:

Co najmniej jeden raz na każde 3 miesiące, użytkownik lub właściciel powinien zapewnić, aby specjalista:

- sprawdził wszystkie zapisy w książce pracy i podjął niezbędne działania, aby doprowadzić do prawidłowej pracy instalacji,
- spowodował zadziałanie, co najmniej jednej czujki lub ręcznego ostrzegacza pożarowego w każdej strefie, w

celu sprawdzenia czy centrala sygnalizacji pożarowej prawidłowo odbiera i wyświetla określone sygnały, emituje alarm akustyczny oraz uruchamia wszystkie inne urządzenia ostrzegawcze i pomocnicze,
- sprawdził, czy monitoring uszkodzeń centrali sygnalizacji pożarowej funkcjonuje prawidłowo,
- w miarę możliwości spowodował zadziałanie każdego łącza do straży pożarnej lub do zdalnego centrum stałej obserwacji,
- przeprowadził wszystkie inne kontrole i próby, określone przez wykonawcę, dostawcę lub producenta,
- dokonał rozpoznania, czy w budynku nastąpiły jakieś zmiany budowlane lub w jego przeznaczeniu, które mogły by wpłynąć na rozmieszczenie czujek i ręcznych ostrzegaczy pożarowych oraz sygnalizatorów akustycznych i – jeśli tak – dokonał oględzin.

Każda zauważona nieprawidłowość powinna być odnotowana w książce pracy i możliwie szybko usunięta.

Obsługa roczna:

Co najmniej jeden raz w roku, użytkownik lub właściciel powinien zapewnić, aby specjalista:
- przeprowadził próby zalecane dla obsługi codziennej, miesięcznej i kwartalnej,
- sprawdził każdą czujkę na poprawność działania zgodnie z zaleceniami producenta (chociaż każda czujka powinna być sprawdzana raz w roku, dopuszcza się sprawdzanie kolejnych 25% czujek przy kolejnej kontroli kwartalnej),
- sprawdził zdolność centrali sygnalizacji pożarowej do uaktywnienia wszystkich funkcji pomocniczych,
- sprawdził wzrokowo, czy wszystkie połączenia kablowe i sprzęt są sprawne, nieuszkodzone i odpowiednio zabezpieczone,
- dokonał oględzin, czy w budynku nastąpiły jakieś zmiany budowlane lub w jego przeznaczeniu, które mogłyby wpłynąć na rozmieszczenie czujek i ręcznych ostrzegaczy pożarowych oraz sygnalizatorów akustycznych. Oględziny powinny także potwierdzić, czy pod każdą czujką jest utrzymana wolna przestrzeń co najmniej 0,5 m we wszystkich kierunkach i czy wszystkie ręczne ostrzegacze pożarowe są dostępne i widoczne,
- sprawdził i przeprowadzić próby wszystkich baterii akumulatorów.

Każda zauważona nieprawidłowość powinna być odnotowana w książce pracy i możliwie szybko usunięta.

Dokumentacja:

Po zakończeniu przeglądu kwartalnego i rocznego, jednostka odpowiedzialna, za przeprowadzenie próby powinna dostarczyć osobie odpowiedzialnej, z potwierdzeniem odbioru, protokół stwierdzający, że próby wymienione w instrukcji zostały wykonane i, że o wykrytych wadach została powiadomiona osoba odpowiedzialna.

4.15 Dobór kabli i przewodów

Wymagania w zakresie kabli i przewodów w systemie SSP:

Typ linii kablowej	**Opis zespołu kablowego**	**Przykładowe rozwiązanie**
Zasilanie centrali CSP	Zespół kablowy: przewód o odporności ogniowej 90 minut + mocowania o odporności ogniowej 90 minut. Mocowania przytwierdzone do podłoża o odpowiedniej odporności ogniowej.	HDGs PH90, NHXH E90 z odpowiednimi mocowaniami o odporności ogniowej 90 minut
Pętle dozorowe / linie konwencjonalne w przestrzeniach nienadzorowanych przez SSP, wewnątrz budynków. Elementy wspólne pętli dozorowej biegnące razem jednym torem/kanałem/przepustem.	Elementy pętli biegnące przez przestrzenie nienadzorowane przez system SSP należy wykonać przewodem PH90 z mocowaniami o odporności ogniowej 90 minut. Mocowania przytwierdzone do podłoża o odpowiedniej odporności ogniowej. Zachować ciągłość ekranu.	HtKSH PH90 1x2x0,8 ekw. z odpowiednimi mocowaniami o odporności ogniowej 90 minut
Pętle dozorowe / linie	Linie dozorowe zewnętrzne (przejścia	XzTKMXpw

konwencjonalne na zewnątrz budynków	pomiędzy budynkami) wykonać przewodem odpornym na wilgoć i promienie UV	
Linie sterujące z modułów	Przewód o odporności ogniowej 90 minut + obejmy o odporności ogniowej 90 minut. Mocowania przytwierdzone do podłoża o odpowiedniej odporności ogniowej.	HtKSH PH90 1x2x0,8 ekw. z odpowiednimi mocowaniami o odporności ogniowej 90 minut

5. System teleinformatyczny

5.1 Założenia projektowe

- W budynku projektuje się instalację teleinformatyczną zadaniem której będzie umożliwienie dostępu wszystkich użytkowników do instalacji telefonicznej oraz instalacji komputerowej.
- Projektuje się dwa główne punkty dystrybucyjne GPD-A (budynek przy ul. Astronomów) i GPD-C (budynek przy ul. Ciołka) okablowania strukturalnego dla jednego i drugiego budynku, które będą się znajdować w pomieszczeniach serwerowni znajdujących się na poziomie +1 każdego z budynków.
- Na kondygnacji -1 w pomieszczeniach przyłączy teletechnicznych znajdują się istniejące przyłącza operatorów telekomunikacyjnych. Projektuje się połączenie teleinformatyczne pomiędzy budynkami. Trasa połączenia widoczna jest na rysunku z planem zagospodarowania terenu.
- Zgodnie ze wskazaniem inwestora projektuje się oddzielną szafę PPD w serwerowni dla wszystkich pomieszczeń Izby Wyższej Urzędu w budynku przy ul. Astronomów na poziomie +3 oraz +4
- Siec LAN wykonana zostanie w technologii Ethernet. Połączenia pomiędzy punktami dystrybucyjnymi (PD i PPD), a głównymi punktami dystrybucyjnymi sieci (GPD1 i GPD2) zostaną zrealizowane z przepływnością 10Gbit/s. Porty przeznaczone dla użytkowników będą pracować w standardzie 10/100/1000 Mb/s
- Przełączniki będę znajdowały się w dwóch głównych punktach dystrybucyjnych (GPD1 na 1 piętrze budynku na ul. Ciołka oraz GPD2 na 1 piętrze budynku na ul. Astronomów) – po jednym w każdym z budynków oraz jednego pośredniego punktu dystrybucyjnego (PPD, na 3 piętrze budynku przy ul. Astronomów).
- Wszystkie produkty wchodzące w skład systemu okablowania strukturalnego muszą pochodzić z oferty jednego producenta.
- Użyte elementy z oferty producenta winny być oznaczone logo tego samego producenta.
- Producent okablowania strukturalnego musi udzielić min. 25 gwarancji na oferowany system zabezpieczając Użytkownika przed nieprawidłowym działaniem poszczególnych komponentów i problemami instalacyjnymi.
- Producent okablowania strukturalnego musi legitymować się ważnym certyfikatem systemu zarządzania ISO9001 od minimum 10 lat, co gwarantuje Użytkownikowi właściwą obsługę procesów sprzedażowych i utrzymaniowych.
- Produkty tworzące tor transmisyjny muszą posiadać właściwe certyfikaty stwierdzające ich zgodność z normami referencyjnymi wskazanymi w punkcie 4.1.2.
- Zakłada się, iż środowisko pracy okablowania będzie środowiskiem łagodnym tj. określonym jako M1I1C1E1 wg. skali MICE zgodnie z EN 50173-1 : 2012.
- Podsystem okablowania poziomego zostanie zrealizowany na bazie systemu ekranowanego o wydajności klasy EA/ kat.6A zgodnie z ISO/IEC 11801 Ed.2.2: 2011 oraz EN 50173-1:2012, co musi zostać potwierdzone certyfikatem niezależnego laboratorium np. Delta, GHMT, itp.;
- Podsystem okablowania pionowego w części światłowodowej oparty zostanie na okablowaniu wielomodowy (zwanym dalej MM). Okablowanie MM charakteryzować się będzie wydajnością OF-300 oraz kategorią włókien OM3 według ISO/IEC 11801 Ed.2.2: 2011. Interfejsem światłowodowym dedykowanym w całej sieci jest LC duplex.
- Poszczególne punkty dystrybucyjne zostały zaprojektowane zgodnie z ISO/IEC 11801 Ed.2.2: 2011.
- Punkty dystrybucyjne oparto na szafach serwerowych 19”, 42U o wymiarach 800x1000 mm, drzwi przednie i tylne z perforacją, boki blaszane pełne
- Zastosowany system okablowania strukturalnego musi charakteryzować się najwyższą elastycznością niezbędna dla ewentualnych rozbudów sieci w czasie użytkowania oraz walorami użytkowymi pozwalającymi na bezproblemową i bezpieczną obsługę systemu przez użytkownika.

- Producent okablowania strukturalnego musi posiadać w ofercie system inteligentnego zarządzania infrastrukturą pasywną oraz umożliwiać rozbudowę systemu okablowania strukturalnego do tej funkcjonalności bez konieczności wymiany paneli oraz kabli krosowych.
- Budowa systemu ma gwarantować możliwość logicznej rekonfiguracji łącza tak, aby mogło one obsługiwać minimum trzy usługi bez konieczności burzenia zbudowanego, pomierzonego i certyfikowanego wcześniej kanału transmisyjnego.
- Budowa systemu ma gwarantować możliwość zmiany interfejsu tak, aby umożliwić w ramach jednej skrętki jednoczesną obsługę 3 usług tj. transmisji danych, telefonii analogowej i CATV. Zmiana taka nie może ciągnąć za sobą zmian warunków gwarancji i konieczności powtarzania pomiarów. Zmiana interfejsu nie może powodować zmiany stałego zakończenia kabla i jego „rozszycia"

Zaprojektowane rozwiązanie teleinformatyczne jest zgodne z Rozporządzeniem Rady Ministrów z dnia 14 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Serwer teleinformatyczny musi umożliwiać natychmiastowe podłączenie do Systemu zarządzania siecią (NMS) wraz z Systemem kontroli dostępu (NAC) realizującego powyższe wymagania.

W szczególności System zarządzania siecią (NMS) wraz z System kontroli dostępu (NAC) przy współpracy z oferowanym serwerem teleinformatycznym musi zapewnić:

1) Zintegrowane zarządzanie urządzeniami IP (telefony IP),
2) Centralne zarządzanie wersjami oprogramowania telefonów i ich aktualizacje, zarządzanie konfiguracją, inventory management, zarządzanie bezpieczeństwem i usługi dla użytkowników końcowych takie jak:
   a) automatyczna transmisja wszystkich parametrów wymaganych przez urządzenie w momencie pierwszego podłączenia do sieci,
   b) zachowanie wszystkich ustawień osobistych użytkownika (jak układ klawiszy, książka telefoniczna, listy połączeń, tony dzwonka, wygaszacz ekranu) i udostępnienie ich w momencie gdy użytkownik loguje się do dowolnego telefonu.
   c) dynamiczna konfiguracja telefonu IP w zależności od lokalizacji telefonu w sieci IP.
   d) wybór trybu aktualizacji wersji oprogramowania telefonu IP:
      - w pełni automatyczny (w przypadku stwierdzenia innego niż dopuszczalne oprogramowania telefon kierowany jest do kwarantanny, automatycznie jest aktualizowane oprogramowanie telefonu po czym telefon powraca z kwarantanny do normalnego trybu pracy),
      - manualny – konieczne działanie administratora po stwierdzeniu niezgodności.
3) W systemie zarządzania w tej samej tabeli są dostępne pola z następującymi danymi:
   a) Numer telefonu,
   b) Adres IP telefonu i MAC adres telefonu,
   c) Nazwa przełącznika do którego podłączony jest telefon i adres IP przełącznika,
   d) Numer portu na przełączniku,
   e) lokalizacja (budynek, pokój, numer gniazdka),
   f) wersja oprogramowania telefonu,
   g) polityka (profil) przypisana do telefonu przez system NAC

Funkcja	**Opis**
Automatyczna Inwentaryzacja	Automatyczna inwentaryzacja zapewnia informację o tym jaki telefon IP został włączony do sieci, jaka jest jego konfiguracja oraz gdzie jest zlokalizowany. Funkcja pozwala na kontrolę wszystkich zmian i przeniesień w ramach sieci.
Automatyczne dopasowanie	System zarządzania może wykorzystać informacje dotyczące danego telefonu do automatycznej rekonfiguracji w zależności od jednego z następujących parametrów: lokalizacja/wersja/model.
Monitoring telefonów IP	Przekazywanie informacji na temat wersji oprogramowania do nadrzędnego systemu zarządzania siecią w celu skierowania telefonów o nieaktualnej wersji oprogramowania do kwarantanny oraz możliwość generowania alertów do administratora w przypadku

	niezgodności
Automatyczna informacja i powiadamianie o błędach	Informacja do użytkownika telefonu o błędzie uwierzytelnienia lub negatywnej weryfikacji zgodności z polityką bezpieczeństwa
Usługa lokalizacji fizycznej	Informacja dla administratora na którym porcie przełącznika został podłączony dany telefon.
Automatyczna autoryzacja	Dynamiczne przydzielenie odpowiedniego VLAN'u w raz z poziomem QoS i ustawieniami bezpieczeństwa
Ciągły monitoring telefonów IP	Informacja dla użytkownika telefonu o przeniesieniu telefonu do kwarantanny na skutek wykrycia ataku przez systemy detekcji intruzów (IDP) oraz system korelacji informacji i przepływów(SIEM)

5.2 Elementy pasywne

5.2.1 Podsystem okablowania pionowego (szkielet)

Połączenie szkieletowe światłowodowe

Światłowodowe połączenia szkieletowe dedykowane są do obsługi protokołów transmisji danych. Na potrzeby niniejszego projektu założono realizację tych połączeń poprzez standardowe połączenia oparte na kablu instalacyjnym poprzez spawanie włókien.

Instalacyjny kabel światłowodowy

W celu umożliwienia realizacji światłowodowych połączeń szkieletowych, pionowy podsystem okablowania strukturalnego został oparty na kablu spełniającym wymagania zebrane w poniższej tabeli.

Kat. kabla wg ISO11801 ed.2.2	OM3 (12 włókien)
Konstrukcja kabla wg DIN VDE 0888	I/A-DQ(ZN=B)H
Powłoka zewnętrzna	Uniwersalna
Budowa kabla	Luźna tuba
Taśma absorbująca wilgoć	Tak
Ochrona przeciw gryzoniom	Tak
Wzmocnienie kabla	Włókno szklane
Klasyfikacja ogniowa powłoki zew.	LSZH
Standardy klasyfikacji ogniowej:	IEC 60332-1 test na rozchodzenie się ognia IEC 60754-2 test na stopień kwasowości gazów IEC 61034 test na gęstość zadymienia

Światłowodowe panele krosowe

Wyspecyfikowane powyżej kable światłowodowe należy właściwie wprowadzić i zaterminować w panelach światłowodowych. Panele muszą charakteryzować się szeregiem własności funkcjonalno użytkowych pozwalających na sprawne, wygodne i oszczędne użytkowanie systemu okablowania przez cały okres jego eksploatacji:

- Panele światłowodowe muszą umożliwiać bezpieczne zrobienia rezerwy ok 2 metrów luźnej tuby w granicach swojej konstrukcji, tak żeby pole spawów i krosowe było odseparowane od miejsca składowania rezerwy
- Panele światłowodowe w swojej przestrzeni muszą być wyposażone w elementy umożliwiające bezpieczne zainstalowanie pigtaili o długości min 2m
- Panel światłowodowy musi stanowić element systemu bezpiecznego prowadzenia kabla instalacyjnego od miejsca jego wprowadzenia do szafy aż do wejścia do panela
- Z uwagi na wykonywanie spawania pigtaile powinny się charakteryzować konstrukcją półścisłej tuby ułatwiającej zdejmowanie zewnętrznego bufora

- Pokrycie wtórne pigtaili musi być różnobarwne dla łatwej identyfikacji w trakcie prac monterskich.
- Pigtaile muszą być ułożone w panelu zgodnie z normą DIN VDE0888, podłączone do adapterów oraz wprowadzone to tacki spawów aby maksymalnie skrócić czas instalacji.
- Panele muszą umożliwiać swobodny dostęp do części połączeniowej oraz pola spawów bez narażania rezerwy luźnej tuby na naprężenia mogące spowodować jej pęknięcie
- Zakłada się możliwość zakończenia w panelu do 24 włókien światłowodowych w przestrzeni pojedynczej jednostki (1U) zakończonych adapterem typu LC/PC duplex.
- Panele muszą mieć możliwość terminowania mniejszej ilości włókien z jednoczesnym zapewnieniem późniejszej ekspansji aż do docelowej ilości 48 włókien
- Panele muszą stanowić kompletne rozwiązanie gotowe do wykonania spawów i ułożenia kabli wewnątrz przełącznicy. W skład kompletu muszą wejść:
    - komplet pigtaili
    - komplet adapterów połączeniowych
    - tacki spawów
    - magazynki spawów
    - komplet osłonek termokurczliwych lub alternatywnych
    - system organizacji zapasu pigtaili
    - system zapewniający bezpieczne wprowadzenia kabla do przełącznicy
- Konstrukcja paneli światłowodowych musi gwarantować nieprzekroczenie dozwolonych promieni gięcia kabli krosowych zabezpieczając je przed naprężeniami, w szczególności przed zgięciem/przytrzaśnięciem przez drzwi szafy.
- Panel musi umożliwiać rozbudowę w elementy systemu zdalnego monitorowania połączeń bez konieczności rozłączania działających połączeń.
- Wymagane parametry adapterów światłowodowych:
    - Zastosowane w adapterach połączeniowych tuleje powinny być ceramiczne co poprawia mechaniczne własności adaptera (niezawodność, dwukrotnie większa żywotność) oraz poprawia własności optyczne całego połączenia.
    - Adaptery światłowodowe muszą być wyposażone w półprzeźroczyste zaślepki przeciwkurzowe, które pod wpływem oświetlenia toru transmisyjnego źródłem światła widzialnego zmieniają kolor, znacznie ułatwiając identyfikację połączeń bez ryzyka uszkodzenie wzroku osoby z obsługi serwisowej.
    - W celu poprawienia obsługi i bezpieczeństwa połączeń, adaptery światłowodowe muszą zapewniać kodowanie kolorem oraz zabezpieczenie złączy przed nieautoryzowanym dokonaniem połączenia oraz rozłączenia
    - Kolorystyka adapterów połączeniowych będących na wyposażeniu paneli ma umożliwiać identyfikację kabli światłowodowych i być zgodna z ISO11801 ed.2.2 tj:
        - Dla włókien wielomodowych turkusowy (OM3

- Wymagane parametry złącz światłowodowych
    - Złącza światłowodowe są kluczowym elementem światłowodowego toru transmisyjnego. Z tego powodu muszą charakteryzować się szeregiem właściwości, które zagwarantują użytkownikowi, z jednej strony taki poziom wydajności, który umożliwi obsługę żądanych aplikacji transmisji danych a z drugiej własności mechaniczne zapewniające bezpieczne użytkowanie sieci. Poniżej zestawiono żądane cechy dla złączy światłowodowych:
    - Zastosowane w panelach złącza muszą charakteryzować się wartościami IL (strata wtrąceniowa) oraz RL (strata odbiciowa) zgodnie z ISO/IEC 11801 ed. 2.2. mierzonych metodą zgodnie z IEC 61300-3-34 dla IL oraz IEC 61300-3-6 dla RL
    - Ferule złączy powinny być ceramiczne co poprawia mechaniczne własności adaptera (niezawodność, dwukrotnie większa żywotność) oraz poprawia własności optyczne całego połączenia
    - Złącza światłowodowe muszą charakteryzować się następującymi parametrami wydajnościowymi zgodnie z IEC 61300-3-34 oraz IEC 61300-3-6

Rodzaj obsługiwanych włókien	wielomodowe
Klasyfikacja złączy wg IEC 61753-1	B_M
Średnie straty wtrąceniowe (IL)[dB] zgodnie z IEC 61300-3-34	≤0,15

Straty wtrąceniowe (RL)[dB] Zgodnie z IEC 61300-3-6	≥35

Wymagane minimalne parametry złącz światłowodowych

5.2.2 Podsystem okablowania poziomego

Łącza transmisyjne dla poziomego podsystemu okablowania zaprojektowana wg modelu Interconnect – TO (2 złączowy) zgodnie z ISO 11801 ed.2.2. Połączenia te realizowane są za pomocą okablowania miedzianego pozwalającego uzyskać wydajność klasy EA. Szczegółowe wymagania dla tego podsystemu zawarte są poniżej:

Miedziane kable instalacyjne

Okablowanie poziome będzie realizowało transmisję danych pomiędzy Piętrowym Punktem Dystrybucyjnym a gniazdami końcowymi. Połączenia poziome miedziane powinny zostać zbudowane w oparciu o kabel typu skrętka miedziana, 4-parowa o wydajności kategorii 6A.

Szczegółowe wymagania dla kabla zawiera poniższa tabela:

Kategoria	Kat.6A
Częstotliwość	650 MHz
Konstrukcja kabla	S/FTP
Zgodność z aplikacjami	IEEE 802.3an; 10Base-T; 100Base-TX; 1000Base-T; 10GBase-T IEEE 802.5 16MB; ISDN; TPDDI; ATM
Zgodność ze standardami	ISO/IEC 11801 Ed.2 EN 50173-1 IEC 61156-5 Ed.2 EN 50288-10-1
Klasyfikacja ogniowa	LSZH IEC 60332-1; IEC 60754-2; IEC 61034, EN50575
Klasyfikacja ogniowa CPR (EN50575)	Eca
Średnica nominalna kabla max.	7.3 mm

Moduły przyłączeniowe

Moduły przyłączeniowe stanowią jeden z kluczowych elementów okablowania strukturalnego mające bezpośredni wpływ na wydajność łączy. W związku z powyższym muszą spełniać szereg wymagań gwarantujących zachowanie założeń projektowych:

- W ramach całego systemu okablowania strukturalnego dopuszcza się stosowanie jednego rodzaju modułu we wszystkich zastosowanych platformach
- Moduły muszą jednocześnie umożliwiać wprowadzania kabla instalacyjnego na wprost (180˚) oraz prostopadle (90˚), co ma szczególne znaczenie dla gniazd abonenckich gdzie przestrzeń kablowa jest bardzo ograniczona.
- Kategoria zastosowanego miedzianego modułu przyłączeniowego zgodnie z założeniami projektowymi musi spełniać wymagania dla Kat.6A co stanowi podstawę do uzyskania wydajności toru transmisyjnego Klasy EA wg. IEC 11801 ed.2.2., EN50173-1, TIA/EIA 568C. Wydajność ta jest wystarczająca do obsługi aplikacji LAN do 10GBase-T
- Sposób terminacji żył kabla w module musi być wykonany za pomocą technologii IDC, jako powszechnie uznaną za najbardziej niezawodną metodę terminacyjną.
- Dla zachowania elastyczności systemu, moduły muszą jednocześnie mieć możliwość terminacji żył typu drut jak i linka w następujących rozpiętościach średnic:
  - AWG 22- 26 AWG dla drutu
  - AWG 22/7 – 26/7 AWG dla linki
- Moduły muszą obsługiwać możliwie szeroką gamę kabli, stąd niezbędne jest zapewnienie obsługi kabli o średnicy żyły wraz z powłoką aż do min 1.5 mm
- Konstrukcja modułu musi umożliwiać obsługę kabli o średnicy zewnętrznej do 10mm.

- Metoda terminacji kabla instalacyjnego w module musi gwarantować niezależność jakości uzyskanego kontaktu od stanu i jakości samego narzędzia terminującego.
- Moduły muszą pozwalać na terminację kabla w sekwencji TIA/EIA 568A lub B
- Moduł muszą zapewniać ochronę strefy kontaktu poprzez przytwierdzenie kabla instalacyjnego do obudowy modułu.
- Moduły muszą obsługiwać technologię PoE oraz PoE+ (Power Over Ethernet)
- Żyły kabla instalacyjnego muszą być w obrębie kontaktu IDC unieruchomione co zapobiega obruszaniu kontaktu. Ma to szczególne znaczenie w przypadku zastosowania PoE
- Moduły zgodnie z ISO 11801 ed.2.2. muszą zapewniać minimum 20 krotną reterminację. Wymagane jest przedstawienie stosownego raportu z testów.
- Moduły zgodnie z ISO 11801 ed.2.2. muszą zapewniać minimum 750 cykli połączeniowych. Wymagane jest przedstawienie stosownego raportu z testów.
- Dla zagwarantowania właściwych parametrów transmisji piny modułów muszą być pokryte warstwą złota o grubości min 0,7 µm.
- Ekranowanie modułu musi zapewniać ochronę 360˚
- Styk ekranowania kabla instalacyjnego z ekranem modułu musi gwarantować przejście o minimalnej impedancji, czyli powierzchnia samego styku powinna być odpowiednio duża

Miedziane kable krosowe

Miedziane kable krosowe mają za zadanie połączyć sprzęt sieciowy z panelami krosowymi lub gniazdami abonenckimi. Kategoria kabli połączeniowych musi być adekwatna do kategorii komponentów użytych do budowy danego łącza. W związku z powyższym dopuszcza się kable spełniające następujące wymagania:
- Kable krosowe kat.6A muszą być testowane zgodnie z IEC 61935-2.
- Kable muszą prezentować marginesy pracy dla zapewnienia poprawności obsługi wszystkich aplikacji transmisji danych również tych, które zostaną opracowane w przyszłości.
- Kable krosowe, w dowolnym momencie eksploatacji muszą posiadać możliwość doposażenia ich w elementy umożliwiające kodowanie kolorem oraz mechaniczne zabezpieczenia przeciwko nieautoryzowanemu wpięciu i wypięciu złącza kabla z portu.
- Kable krosowe w dowolnym momencie eksploatacji muszą posiadać możliwość doposażenia ich w elementy umożliwiające aktywne monitorowanie stanu połączeń w czasie rzeczywistym.
- Wtyki RJ45 kabli krosowych muszą opierać się na technologii IDC w celu zagwarantowania niezmiennych parametrów pracy w czasie eksploatacji. Nie dopuszcza się technologii Piercing;
- W ramach kontroli jakości produkcji, kable krosowe muszą być sprawdzane w 100%, a nie jedynie na próbkach;

Podstawowe parametry kabli krosowych zawiera poniższa tabela

Kategoria	Kat.6_A
Zakres częstotliwości, w którym badano kable [MHz]	Do 650
Rodzaj powłoki	LSFRZH
Klasyfikacja ogniowa	IEC 60332-3-24; IEC 60754-2; IEC 61034
Ekranowanie	S/FTP
Max ø kabla [mm]	6.0
Średnica przewodu	AWG 26/7

Panele krosowe do obsługi transmisji danych

Wyspecyfikowane powyżej kable miedziane należy właściwie wprowadzić i zaterminować w panelach krosowych. Panele muszą charakteryzować się szeregiem własności funkcjonalno użytkowych pozwalających na sprawne, wygodne i oszczędne użytkowanie systemu okablowania przez cały okres jego eksploatacji:

Panel 1U HD 24 portów (z możliwością rozbudowy do 48 portów):

- Panel musi zajmować 1U miejsca w szafie 19”
- Zagęszczenie portów musi zapewniać obsługę do 48 portów
- Panel musi umożliwiać kodowanie kolorem, co poprawia walory administracyjne rozwiązania
- System w skład, którego wchodzi panel musi zapewniać mechaniczne zabezpieczenie portów przed nieautoryzowanym wpięciem oraz wypięciem złącza do/z gniazda
- Konstrukcja panela musi charakteryzować się elastycznością pozwalającą na przyszłe rozbudowy/migracje sieci, tj. panel musi mieć możliwość obsługiwania:
  - łączy miedzianych kategorii 5,6 lub 6A
  - łączy optycznych minimum SC oraz LC dupleks w wersji pre-terminowanej i spawanej
  - jednoczesnej dowolnej mieszanki wyżej wymienionych łączy
- Konstrukcja panela musi gwarantować możliwość jego obsługi od przodu, co wydatnie usprawnia jego obsługę w sytuacji ograniczonego dostępu do szafy z innych stron
- Panel musi umożliwiać zaimplementowanie systemu inteligentnego monitorowania portów w dowolnym momencie jego użytkowania bez konieczności rozłączania istniejących połączeń
- Panel musi posiadać duże, wymienialne pola opisowe pozwalające na etykietowanie połączeń. Dodatkowo każdy port musi być ponumerowany
- Porty RJ45 przewidziane dla gniazd WIFI oraz kamer CCTV należy zabezpieczyć przed nieautoryzowanym wypięciem patchcordu z portu

Dodatkowo w celu ułatwienia administrowania siecią należy dostarczyć akcesoria kodujące do gniazd, paneli oraz kabli krosowych wyspecyfikowane w zestawieniu materiałów. Kolory akcesoriów należy uzgodnić przed dostawą z Zamawiającym.

5.2.3 Administracja i etykietowanie

Wszystkie kable powinny być oznaczone numerycznie, w sposób trwały, tak od strony gniazda, jak i od strony szafy montażowej zgodnie ze standardem TIA-606-B oraz ISO/IEC TR14763-2-1. Te same oznaczenia należy umieścić w sposób trwały na gniazdach sygnałowych w punktach przyłączeniowych użytkowników oraz na panelach.
Powykonawczo należy sporządzić dokumentację instalacji kablowej zawierającej trasy kablowe i rozmieszczenie punktów przyłączeniowych w pomieszczeniach zgodnie ze stanem rzeczywistym. Do dokumentacji należy dołączyć raporty z pomiarów torów sygnałowych

5.2.4 Wymagania gwarancyjne

Całość rozwiązania ma być objęta jednolitą, spójną 25-letnią gwarancją systemową producenta, obejmującą całą część transmisyjną wraz z kablami krosowymi i innymi elementami dodatkowymi. Gwarancja ma być udzielona przez producenta bezpośrednio klientowi końcowemu.
Gwarancja systemowa musi obejmować:

- gwarancję produktową (Producent zagwarantuje, że jeśli w jego produktach podczas dostawy, instalacji bądź 25-letniego czasu 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 przez okres 25 lat będzie charakteryzował się parametrami transmisyjnymi przewyższającymi wymogi stawiane przez normę ISO/IEC11801 2nd edition:2002 dla klasy EA)

- wieczystą gwarancję aplikacji (Producent zagwarantuje, że jego system okablowania przez okres „życia" zainstalowanej sieci 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 ed.2.2).
- Wymagana gwarancja ma być bezpłatną usługą serwisowa oferowaną Użytkownikowi końcowemu (Inwestorowi) przez producenta okablowania. Ma obejmować swoim zakresem całość systemu okablowania od Głównego Punktu Dystrybucyjnego do gniazda Użytkownika, w tym również okablowanie szkieletowe i poziome. W celu uzyskania tego rodzaju gwarancji cały system musi być zainstalowany przez firmę instalacyjną posiadającą status Partnera uprawniający do wystąpienia do producenta o udzielenie gwarancji systemowej. Powyższe musi być udokumentowane stosownym certyfikatem producenta. Dopuszczane są certyfikaty wydane w języku innym niż polski;
- wykonawca okablowania strukturalnego winien wykazać się udokumentowaną, kompleksową realizacją projektów z zakresu IT - Data i Voice tzn. dostawą sprzętu aktywnego z konfiguracją, wraz z budową infrastruktury pasywnej.

5.2.5 Odbiory

Warunkiem koniecznym dla odbioru końcowego instalacji przez Inwestora jest uzyskanie gwarancji systemowej producenta potwierdzającej weryfikację wszystkich zainstalowanych torów na zgodność parametrów z wymaganiami norm Klasy EA /Kategorii 6A zgodnie z normami referencyjnymi ujętymi w niniejszym opracowaniu.
W celu odbioru instalacji okablowania strukturalnego należy spełnić warunki zawarte w obowiązujących normach.

Dokumentacja powykonawcza musi zostać wykonana i przekazana Inwestorowi. Musi ona zawierać:
- Raporty z pomiarów dynamicznych okablowania,
- Rzeczywiste trasy prowadzenia kabli transmisyjnych poziomych
- Oznaczenia poszczególnych szaf, gniazd, kabli i portów w panelach krosowych
- Lokalizację przebić przez ściany i podłogi.
- Raporty pomiarowe wszystkich torów transmisyjnych należy zawrzeć w dokumentacji powykonawczej i przekazać inwestorowi przy odbiorze inwestycji. Drugą kopię pomiarów (dokumentacji powykonawczej) należy przekazać producentowi okablowania w celu udzielenia inwestorowi (Użytkownikowi końcowemu) bezpłatnej gwarancji

5.3 Elementy aktywne

5.3.1 Budowa systemu

Zakłada się wykorzystanie topologii gwiazdy rozszerzonej. Punktem centralnym sieci LAN jest Główny Punkt Dystrybucyjny – odpowiednio GPD 1 oraz GPD2, w którym zlokalizowany będzie zdublowany przełącznik rdzeniowy wyposażony w zdublowane zasilacze, umożliwiające redundantne podłączenie zarówno Punktów Dystrybucyjnych PD i PPD, urządzeń i systemów związane z telefonią IP jak i pozostałymi usługami (Firewall, serwery).
Każdy z punktów PD zostanie podłączony z GPD poprzez redundantne połączenie światłowodowe wielomodowe, z wykorzystaniem obu przełączników rdzeniowych. Połączenia te będą zrealizowane w technologii 10 Gigabit Ethernet.
Schemat logiczny systemu:

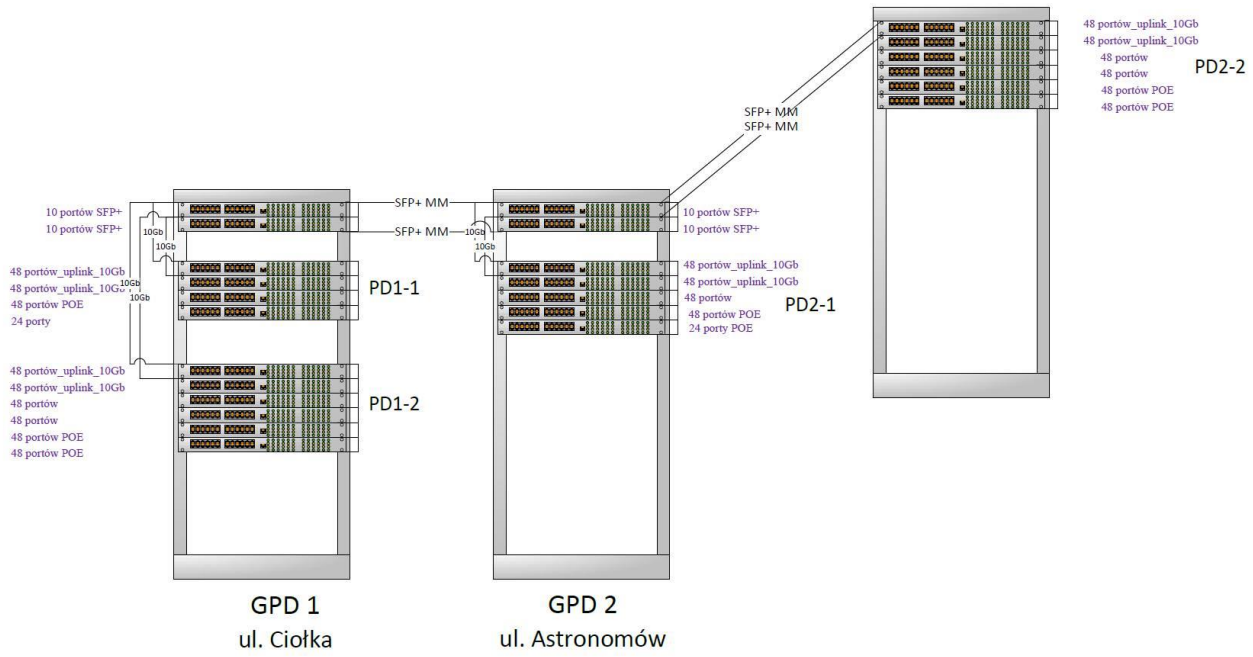


Tabela gniazd dla obiektu:

	Budynek przy ul. Astronomów			Budynek przy ul. Ciołka		
	Gniazda LAN	Gniazda telef.	Gniazda LAN-WiFi	Gniazda LAN	Gniazda telef.	Gniazda LAN-WiFi
Piwnica	4			4		
Parter	72	36		44	14	2
Piętro 1	62	29		62	16	
Piętro 2	60	28		58	27	
Piętro 3	66	31		60	28	
Piętro 4	66	27		68	32	
	330	151	0	296	117	2
	Gn. LAN	Gn. TEL				
	628	268				

Podsumowanie ilości przełączników w poszczególnych stosach / punktach dystrybucyjnych. Kolory oznaczają przyporządkowanie stosów przełączników do poszczególnych punktów dystrybucyjnych

PPD/ Przełączniki	24x1G	48x1G	24x1G_PoE	48x1G_PoE
PD1-1	1	2		1
PD1-2		4		2
PD2-1		3	1	1
PPD2-2		4		2
RAZEM	1	13	1	6

Mechanizmy separacji

Projektowana sieć będzie przenosić ruch związany z działaniem szeregu systemów i różnych grup użytkowników. Konieczne jest zatem zapewnienie separacji ruchu polegającej na zaimplementowaniu mechanizmów separujących ruch dla poszczególnych systemów i grup użytkowników poprzez zastosowanie technologii NAC (Network Access Control).

Zarządzanie urządzeniami aktywnymi

Jednorodna aplikacja dla zarządzania wszystkimi posiadanymi i dostarczanymi urządzeniami sieciowymi jest niezbędna do utrzymania na pożądanym poziomie całej infrastruktury. W szczególności musi umożliwiać zarządzanie urządzeniami aktywnymi, zdalną konfigurację urządzeń, kreowanie spójnej polityki bezpieczeństwa oraz zarządzanie istniejącymi i planowanymi usługami. W związku z powyższym wszystkie dostarczane urządzenia muszą umożliwiać zarządzanie poprzez jednolity system zarządzania siecią, którego szczegółowa funkcjonalność znajduje się w dalszej części.

Bezpieczeństwo transmisji

Z punktu widzenia bezpieczeństwa transmisji danych, konieczne jest zapewnienie możliwie wysokiej dostępności, wydajności i odporności sieci nie tylko w Głównych Punktach Dystrybucyjnych ale również w miarę dostępnych mechanizmów w części dostępowej.

Powyższe założenie rozumiane przez redundancję fizyczną będzie osiągnięte dla GPD poprzez:
- duplikację przełączników rdzeniowych i ich zasilania,
- zwielokrotnienie połączeń w relacjach dotyczących przełączników rdzeniowych – stosów przełączników dystrybucyjnych.

W aspekcie bezpieczeństwa realizowanego na poziomie części dostępowej sieci, transmisja będzie podlegała zabezpieczeniu za pomocą dostępnych standardów szyfrowania świadczonego przez poszczególne urządzenia aktywne dla odpowiednich mediów transmisyjnych. Ponadto muszą zostać zaimplementowane odpowiednie mechanizmy autoryzacji urządzeń i użytkowników dołączanych do sieci w oparciu o komponent umożliwiający realizację systemu kontroli dostępu NAC (Network Access Control).
W tym celu należy zastosować polityki bezpieczeństwa pozwalające na przepuszczanie, blokowanie, ograniczanie poziomu, tagowanie, przekierowywanie i kontrolowanie ruchu sieciowego, w oparciu o tożsamość użytkownika, czas i położenie, typ urządzenia i inne zmienne środowiskowe. Polityki bezpieczeństwa muszą być dynamicznie egzekwowane na poziomie sieci, w szczególności portu przełącznika dostępowego (zalecenie VLAN RFC3580) poprzez zastosowanie technologii NAC dla każdego urządzenia wykorzystującego RADIUS do uwierzytelniania z konfigurowalnymi atrybutami, takimi jak Login-LAT lub Filter ID. Rozwiązanie integrując się z serwerem uwierzytelniającym może wykorzystywać różnego typu polityki zależnie od atrybutu Reject RADIUS. Przykładowo, inna polityka może być zastosowana do użytkownika z wygasłym hasłem niż do użytkownika, który nie posiada konta lub przynależy do innej grupy użytkowników zgodnie z jego rolą organizacyjną.

5.3.2 Wymagania dla urządzeń aktywnych sieci LAN

Punkt centralny (Główny Punkt Dystrybucyjny, GPD1 i GPD2) sieci tworzą pary przełączników rdzeniowych pracujące w warstwie trzeciej, agregujące ruch z punktów dostępowych (PD, PPD) oraz segmentów serwerowni. Wraz z przełącznikami dostarczone zostaną odpowiednie moduły w standardzie SFP+.

W celu uzyskania jak najoptymalniejszej wydajności połączeń, utrzymania oraz dostępności przełączników zlokalizowanych w GPD w PPD, funkcje zarządzania, routingu i łączności pomiędzy lokalizacjami tworzącymi warstwę rdzeniową i dystrybucyjną zapewnione zostaną za pomocą odpowiednich protokołów transmisyjnych oraz duplikacji łączy.

Wyżej opisane Główne Punkty Dystrybucyjne GPD1 i GPD2, będą odpowiedzialne przede wszystkim za wydajną wymianę ruchu pomiędzy poszczególnymi segmentami sieci i stykiem z operatorem zewnętrznym.
Drugim zadaniem GPD, dzięki systemowi kontroli dostępu (NAC) oraz systemowi zarządzania siecią, który musi zostać zainstalowany w dedykowanym środowisku wirtualnym, będzie możliwość zunifikowanego zarządzania wszystkimi posiadanymi i dostarczanymi urządzeniami aktywnymi oraz spójnego egzekwowania polityki

bezpieczeństwa na poziomie portów dostępowych przełączników dla całego ruchu pochodzącego z infrastruktury dostępowej.

W związku z zaawansowanym wykorzystaniem różnorodnych aplikacji związanych z charakterystyką środowiska informatycznego Zamawiającego, funkcjonalność systemu informatycznego musi dostarczać dane na temat sposobu wykorzystania tych aplikacji w ramach lokalnych zasobów informatycznych. W tym celu musi zostać zapewniona widoczność sieci i działania aplikacji, pozwalając na wskazywanie i rozwiązywanie problemów z wydajnością infrastruktury, niezależnie od tego czy są one spowodowane przez sieć, aplikacje czy środowisko serwerów.

Aby zapewnić właściwą wydajność oraz elastyczność przy zarządzaniu rozkładem ruchu w sieci, połączenia dystrybucyjne pomiędzy GPD a PD (PPD) powinny być realizowane w oparciu o zagregowane łącza 2 x 10 Gigabit Ethernet. Wraz z przełącznikami dostarczone zostaną moduły optyczne w standardzie SFP+, przewody do łączenia w stos i kable zasilające.

W skład Głównych Punktów Dystrybucyjnych GPD1 i GPD2 wchodzą dostarczane w bieżącym zamówieniu następujące komponenty aktywne i systemy aplikacyjne sieci:

1. Przełączniki rdzeniowe sieci,
2. System zarządzania siecią (NMS) wraz z Systemem kontroli dostępu (NAC).
3. Kontroler sieci bezprzewodowej WLAN + punkty dostępowe

Połączenia pomiędzy poszczególnymi PD (PPD) a GPD zrealizowane zostaną w technologii optycznej z zapewnieniem przepustowości 2x10 Gbps. Wraz z przełącznikami dostępowymi dostarczone zostaną moduły optyczne w standardzie SFP+, przewody do łączenia w stos i kable zasilające.

Wyposażenie poszczególnych punktów dystrybucyjnych stanowić będą przełączniki dostępowe w liczbie zgodnej z zestawieniem ilościowym. W celu osiągnięcia wymaganej liczby portów dostępowych w poszczególnych PD przełączniki połączone będą w stosy tworząc wirtualny przełącznik oraz zapewniając zintegrowane zarządzanie punktem dystrybucyjnym poprzez pojedynczy adres IP. Dedykowane porty do łączenia w stos poprzez zastosowanie łącza typu backbone muszą zapewnić przepustowość pomiędzy urządzeniami na poziomie 40 Gbps nie konsumując przy tym portów dostępowych przełącznika. Dzięki możliwości łączenia zarówno przełączników wyposażonych w 24, jaki 48 portów pojedynczy stos może być rozbudowywany w miarę rosnącego zapotrzebowania na porty dostępowe.

5.3.3 Wymagania dla urządzeń typu przełącznik

Każdy z przełączników musi realizować co najmniej poniższe funkcjonalności:

1. Wysokość urządzenia 1U
2. Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az na wszystkich portach 10/100/1000BASE-T
3. Wbudowany dodatkowy interfejs do zarządzania poza pasmem - out of band management.
4. Przełącznik musi posiadać wbudowany zasilacz 230V AC, oraz musi posiadać możliwość realizacji redundancji zasilania poprzez instalację wewnętrznego lub zewnętrznego dodatkowego zasilacza.
5. Możliwość łączenia do 8 przełączników w stos. Dodatkowo musi posiadać możliwość realizacji stosów z wykorzystaniem wbudowanych portów 10G na duże odległości za pomocą standardowych wkładek 10GBase-SR/LR oraz włókien światłowodowych
6. Tablica MAC adresów min. 16k
7. Pamięć operacyjna: min. 1GB pamięci DRAM
8. Pamięć flash: min. 4GB pamięci Flash oraz bufora pakietów min. 1,5MB
9. Port USB min. 2.0 przeznaczony do celów serwisowych
10. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
11. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
12. Obsługa Quality of Service (IEEE 802.1p, DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym)
13. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
14. Możliwość monitorowania zajętości CPU

Obsługa Routingu IPv4:

15. Pojemność tabeli routingu min. 480 wpisów
16. Routing statyczny

17. Obsługa routingu dynamicznego IPv4: RIPv1/v2 lub możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania
18. Policy Based Routing dla IPv4

Obsługa Routingu IPv6:

19. Pojemność tabeli routingu min. 240 wpisów
20. Routing statyczny
21. Obsługa routingu dynamicznego dla IPv6
a. RIPng
b. Możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla OSPFv3 (np. poprzez dodatkową licencję)
22. Policy Based Routing dla IPv6

Obsługa Multicastów:

23. Obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration)
24. Obsługa IGMP v1v2/v3 oraz IGMP v1/v2/v3 snooping

Bezpieczeństwo:

25. Obsługa Network Login
a. IEEE 802.1x
b. Web-based Network Login
c. MAC based Network Login
26. Obsługa wielu klientów (min. 8) Network Login na jednym porcie (Multiple supplicants)
27. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z systemu NAC
28. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
29. Musi działać w architekturze bezpieczeństwa opartej o role. Zapewniając ciągłe zarządzanie tożsamościami z uwierzytelnianiem opartym o role, autoryzacją, QoS i ograniczaniem poziomu pasma
30. Urządzenie musi wspierać profile bezpieczeństwa definiowane per użytkownik. Profil bezpieczeństwa oznacza połączenie:
a. definicji sieci VLAN,
b. reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,
c. realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,
d. realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.
31. Obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) – również per-command Authentication
32. Bezpieczeństwo MAC adresów
a. ograniczenie liczby MAC adresów na porcie
b. zatrzaśnięcie MAC adresu na porcie
c. możliwość wpisania statycznych MAC adresów na port/vlan
d. możliwość wyłączenia MAC learning
33. Zabezpieczenie przełącznika przed atakami DoS
a. Networks Ingress Filtering RFC 2267
b. SYN Attack Protection
c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
34. Dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika)
35. Obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation
36. Obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard

Bezpieczeństwo sieciowe:

37. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania
38. Obsługa STP, RSTP, MSTP, PVST+
39. Obsługa EAPS (RFC 3619) oraz G.8032
40. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów
41. Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników.

Zarządzanie:

42. Zarządzanie przez SNMP v1/v2/v3
43. Obsługa SYSLOG z możliwością definiowania wielu serwerów
44. Sprzętowa obsługa sFlow
45. Obsługa RMON (RFC 1757) i RMON2 (RFC 2021)

Inne
46. Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych)
47. Możliwość uruchamiania skryptów
a. Ręcznie
b. O określonym czasie lub co wskazany okres czasu
c. Na podstawie wpisów w logu systemowym

UWAGA: wymagania szczegółowe dla wszystkich typów przełączników zawarto w specyfikacji technicznej projektu wykonawczego dla branży niskoprądowej

5.3.4 Kontroler sieci WLAN

Kontroler sieci WLAN musi posiadać wsparcie producenta w zakresie pomocy technicznej 24x7x365 oraz aktualizacji oprogramowania na okres 36 miesięcy. Dodatkowo dostęp do bazy wiedzy producenta, która zapewnia bezpośredni dostęp np. do dokumentacji. W przypadku rozwiązania sprzętowego – wymiana uszkodzonego sprzętu musi zostać wykonana następnego dnia roboczego po zgłoszeniu awarii.

Architektura
Kontroler sieci bezprzewodowej w momencie dostawy musi obsługiwać minimum 8 punktów dostępowych. Kontroler musi umożliwiać docelową rozbudowę do minimum 150 punktów dostępowych poprzez zakup dodatkowych licencji.
Kontroler musi obsługiwać jednocześnie różne mechanizmy przekazywania danych, w tym tunelowanie ruchu z AP do kontrolera i lokalnego terminowania do sieci przewodowej na poziomie AP (mechanizmy te muszą być dostępne do skonfigurowania w obrębie tego samego kontrolera, per SSID)

Captive Portal:

1. Kontroler sieci WLAN musi przekierowywać użytkowników określonych SSID do strony logowania (z możliwością personalizacji strony)
2. Musi posiadać zintegrowany (w kontrolerze), logicznie wydzielony portal dostępowy (Captive Portal), dowolnie konfigurowany przez administratora, z wykorzystaniem wbudowanych narzędzi edycyjnych
3. Dostęp gościnny poprzez Captive Portal musi umożliwiać logowanie do sieci WLAN z wykorzystaniem autentykacji 802.1x
4. Możliwość kreowania użytkowników za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta
5. Captive Portal musi dawać dostęp Gościom do zasobów sieci Internet w dedykowanym VLAN-nie (Sieć Gości), nie dopuszczając Gości do zasobów wewnętrznych Zamawiającego (Intranet).
6. Możliwość kreowania różnych polityk bezpieczeństwa w ramach pojedynczego SSID
7. Możliwość profilowania użytkowników – co najmniej przydział: sieci VLAN, list kontroli dostępu (ACL), mechanizmów QoS, 802.1p, oraz ograniczanie pasma per użytkownik

Bezpieczeństwo:

8. Musi obsługiwać IP QoS w środowisku przewodowym i bezprzewodowym. Rozróżnianie pakietów musi być realizowane dla przychodzących i wychodzących pakietów z sieci bezprzewodowej, w oparciu o 802.1p
9. Musi umożliwiać automatyczną ochronę kryptograficzną (AES) ruchu pomiędzy punktem dostępowym, a Kontrolerem WLAN.
10. System musi obsługiwać kreowanie polityk bezpieczeństwa w obrębie jednego SSID (przypisywanie indywidualnych parametrów obsługi ruchu poszczególnym użytkownikom VLAN, QoS, ACL, ograniczenie

pasma), bez konieczności segmentacji przez dedykowane SSID. Rozwiązanie powinno w ten sposób zmniejszyć konieczność uruchomienia wielu SSID do realizowania różnych funkcjonalności (minimalizacja utylizacji pasma radiowego)

Zarządzanie:

11. Musi umożliwiać zarządzanie poprzez ssh, https, snmpv3 oraz dedykowaną aplikację do zarządzania.
12. Wraz z rozwiązaniem wymaga się dostarczenia rozwiązania do zarządzania i monitorowania kilkoma kontrolerami sieci WLAN – centralny interfejs graficzny.
13. Musi umożliwiać optymalizację wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany).
14. W przypadku awarii punktu dostępowego, sąsiednie punkty dostępowe muszą rozszerzyć swój zasięg by wyeliminować niepokryte obszary, nawet w sytuacji, gdy punkt dostępowy nie może uzyskać dostępu do kontrolera. Wybór optymalnego kanału musi także być rekonfigurowany dynamicznie, bez interwencji użytkownika.
15. System zarządzania łącznością radiową RF Management musi dostosowywać się do nowych kanałów w oparciu o wartości stosunku sygnału do szumu (SNR) i zajętości kanału, które mogą być ustalane przez użytkownika.
16. Musi mieć możliwość zapewnienia równego czasu antenowego (Airtime) dla wszystkich klientów w środowiskach, w których wspólnie występują technologie 802.11ag oraz 802.11n. (rozwiązanie Airtime fairness, np. ClientLink lub równoważne). System zarządzania łącznością radiową – typu RRM (Radio Resource Management) - RF Management musi wspierać funkcje automatycznego wyboru kanału i automatycznej kontroli mocy emitowanego sygnału TPC (Transmit Power Control) oraz obsługa Dynamic Frequency Selection (DFS).
17. Kontroler musi zapewniać zarządzanie oparte o graficzny interfejs użytkownika, lokalny uruchomiony na kontrolerze WLAN.
18. Musi pozwalać nietechnicznym pracownikom na tworzenie tymczasowych kont gości i dystrybuowanie zezwoleń poprzez łatwy w użyciu graficzny interfejs użytkownika – dla celów Captive Portal.

System WIPS/WIDS:

19. Kontroler musi oferować funkcje WIPS/WIDS, działające bez wpływu na poziom świadczonych usług sieciowych co oznacza, że muszą być dostępne zarówno funkcje wykrywania, jak i zmniejszania zagrożeń, gdy punkt dostępowy świadczy innym klientom sieci bezprzewodowej usługi transmisji danych.
20. Wymagane jest scentralizowane raportowanie i konfiguracja WIPS/WIDS, z kilku kontrolerów WLAN jednocześnie.

UWAGA: wymagania szczegółowe dla kontorlerów zawarto w specyfikacji technicznej projektu wykonawczego dla branży niskoprądowej

5.3.5 Punkt dostępowy sieci WLAN

Pasma robocze:
1. Punkty dostępowe muszą posiadać min. 2 moduły radiowe i obsługiwać równolegle dwa pasma częstotliwości: (2,4 GHz) 802.11b/g/n oraz (5GHz) 802.11a/n/ac Wave 2

Interfejsy fizyczne:
2. Punkty dostępowe muszą być wyposażone w 2 porty 10/100/1000 BASE-T RJ-45

Standardy sieciowe:
3. Zgodność z DFS2 (Dynamic Frequency Selection)
4. Punkty dostępowe muszą obsługiwać IP QoS w środowisku przewodowym i bezprzewodowym. Rozróżnianie pakietów musi być realizowane dla przychodzących i wychodzących pakietów z sieci bezprzewodowej, w oparciu o DiffServ, IP ToS oraz IP Precedence,

5. Szybki i bezpieczny roaming oraz handover (wstępne uwierzytelnienie, OKC)
6. Obsługa do 16 SSID (8 na częstotliwość radiową),
7. Obsługa minimum 450 użytkowników jednocześnie,
8. RADIUS Authentication & Accounting,
9. Wsparcie dla protokołu IEEE 802.1p prioritization, IEEE 802.1X z wykorzystaniem metod: EAP-SIM, EAPFAST, EAP-TLS, EAP-TTLS, and PEAP,
10. Wsparcie dla protokołu: MAC address authentication przy wykorzystaniu lokalnych access-list lub przesyłanych z serwera RADIUS,
11. Mechanizmy: RADIUS AAA, przy wykorzystaniu EAP-MD5, PAP, CHAP oraz MS-CHAPv2,
12. Mechanizm izolacji klientów na poziomie L2,
13. Mechanizmy IEEE 802.11i, WPA2 oraz WPA, przy zastosowaniu algorytmów szyfracji: Advanced Encryption Standard (AES) oraz Temporal Key Integrity Protocol (TKIP),
14. Musi mieć możliwość zapewnienia równego czasu antenowego (Airtime) dla wszystkich klientów w środowiskach, w których wspólnie występują technologie 802.11a/b/g, 802.11n oraz 802.11ac.

Anteny:

15. Muszą posiadać min. 8 anten wewnętrznych.

Tryby pracy:

16. Tryb działania radio WLAN: Client access, Local mesh, Packet capture, WDS,
17. Możliwość pracy punktu dostępowego bez kontrolera WLAN na wypadek awarii łącza,
18. Możliwość pracy punktu dostępowego z rozwiązaniem chmurowym (Cloud) producenta, poprzez wykupienie odpowiedniej subskrypcji/licencji,
19. Obsługa technologii 802.11ac i praca w technice transmisji wieloantenowej MIMO 4x4:4
20. Obsługa 802.11n z przepływnością do co najmniej 800Mbps i 802.11ac z przepływnością do co najmniej 1,7Gbps
21. Jednoczesna obsługa ruchu tunelowanego i mostowanego,
22. Wszystkie punkty dostępowe muszą mieć możliwość pracy w formie sensorów sieci (sensor działający w kanale pracy i świadczący jednocześnie WiFi dla Klientów, oraz dedykowany sensor skanujący wszystkie kanały w danej częstotliwości radiowej);
23. W przypadku awarii punktu dostępowego, sąsiednie punkty dostępowe muszą rozszerzyć swój zasięg by wyeliminować niepokryte obszary, nawet w sytuacji, gdy punkt dostępowy nie może uzyskać dostępu do kontrolera.
24. Punkt dostępowy w połączeniu z oprogramowaniem do zarządzania powinien umożliwiać wgląd w ruch użytkowników/Klientów do warstwy aplikacji (warstwa 7)

Funkcje zarządzania:

25. Punkt dostępowy musi zapewniać rozproszone zarządzanie łącznością radiową RF (Radio Frequency) Management niezależne od kontrolera - poza tylko wstępną konfiguracją. Po utracie połączenia z kontrolerem, punkt dostępowy musi być zdolny do zapewnienia ciągłości operacji związanych z szyfrowaniem, tworzeniem czarnych list, filtrowaniem, QoS oraz zarządzaniem łącznością radiową, zarówno dla swoich potrzeb, jak i lokalnie mostowanego ruchu.
26. Zarządzanie łącznością radiową RF Management musi dostosowywać się do nowych kanałów w oparciu o wartości stosunku sygnału do szumu (SNR) i zajętości kanału
27. Możliwość konfiguracji zapewniającej równoważenie obciążenia i sterowanie pasmem w celu pozwolenia punktom dostępowym na równoważenie/sterowanie ruchem klientów pomiędzy obiema częstotliwościami na jednym punkcie dostępowym i/lub pomiędzy wieloma punktami dostępowymi w ramach domeny łączności radiowej,

Bezpieczeństwo :

28. Połączenie pomiędzy AP, a kontrolerem musi być szyfrowane przy pomocy technologii AES minimum 128 bit,
29. Punkty dostępowe muszą obsługiwać suplikanta 802.1x, by chronić swoje połączenia przewodowe przed nieautoryzowanym dostępem innych urządzeń,

30. Obsługa standardów uwierzytelniania i szyfrowania, w tym: WEP, WPA (TKIP), WPA2 (AES), 802.11i, 802.1x,
31. Punkt dostępowy musi wspierać szyfrowanie, tworzenie czarnych list, filtrowanie oraz QoS, niezależnie od kontrolera,
32. Możliwość pracy w architekturze bezpieczeństwa opartej na rolach, zapewniając ciągłe zarządzanie tożsamością wraz z opartymi na rolach funkcjami uwierzytelniania, autoryzacji, QoS i ograniczania pasma, aplikowane względem użytkownika i aplikacji,
33. Funkcje egzekwowania przypisanych ról i ograniczania przepustowości muszą być osiągalne na poziomie punktu dostępowego,
34. Przypisywanie ról klientom musi odbywać się bez konieczności segmentacji przez dedykowane SSID.

WIPS:

35. Wymagane jest scentralizowane raportowanie i konfiguracja WIPS/WIDS,
36. Punkt dostępowy musi oferować funkcje WIPS/WIDS, działające bez wpływu na poziom świadczonych usług sieciowych, muszą być dostępne zarówno funkcje wykrywania, jak i zmniejszania zagrożeń, gdy punkt dostępowy świadczy innym klientom Wi-FI usługi transmisji danych
37. Kategorie zagrożeń WIDS/WIPS, które należy wykrywać i raportować:

a. Analizy widma – zakłócenia pochodzące ze źródeł innych niż WiFi,
b. Aktywna obserwacja
c. Atak Packet Injection (wtryskiwanie pakietów) – atakujący wprowadza swoje pakiety w transmisję danych pomiędzy dwoma urządzeniami, dzięki temu urządzenia traktują te złośliwe pakiety, tak jakby pochodziły z autoryzowanego urządzenia,
d. Atak Denial of Service (skierowany na stację końcową) – zalewanie stacji końcowej komunikatami uwierzytelniania lub anulowania uwierzytelniania

38. Kategorie zagrożeń WIDS/WIPS, które należy wykrywać, raportować i zmniejszać:

a. Honeypot
b. Wrogi punkt dostępu (ang. Rogue AP) – punkt dostępowy podłączony do autoryzowanej sieci, pomimo braku upoważnienia do tego,
c. Fałszywy punkt dostępu (ang. Spoofing AP) – urządzenie posługujące się BSSID (adres MAC) w rzeczywistości należącym do innego, autoryzowanego punktu dostępowego,
d. Aktywne łamanie szyfrowania (ang. Active Encryption Cracking) – atak typu chop-chop i fragmentaryczny,
e. Atak Denial of Service (skierowany na punkt dostępu)

Inne:

39. Musi być dostarczony z uchwytem mocującym do powierzchni płaskich (np. ściany), oraz sufitów podwieszanych.

5.3.6 System zarzadzania siecią (NMS)

System zarządzania siecią musi umożliwiać objęcie swoim działaniem wszystkich urządzeń (LAN/WLAN) dostarczanych w ramach postępowania. Musi posiadać wsparcie producenta w zakresie pomocy technicznej 24x7x365 oraz aktualizacji oprogramowania na okres 36 miesięcy. Dodatkowo dostęp do bazy wiedzy producenta, która zapewnia bezpośredni dostęp np. do dokumentacji.
Jeżeli w oferowanym systemie licencje są czasowe, ograniczające w jakikolwiek sposób funkcjonalność rozwiązania, Zamawiający wymaga dostarczenia licencji na okres nie mniejszy niż 10 lat.

Minimalna wymagana funkcjonalność:

1. Musi umożliwiać zbieranie statystyk co najmniej z wykorzystaniem SNMP lub RMON.
2. Musi umożliwiać centralne wykonywanie operacji systemowych, takich jak wykrywanie urządzeń, zarządzanie zdarzeniami, rejestrowanie zdarzeń i utrzymanie aplikacji
3. Musi zapewnić narzędzie umożliwiające szybkie i łatwe określenie fizycznej lokalizacji systemów i użytkowników końcowych oraz miejsca ich podłączenia do sieci (LAN/WLAN)
4. Musi zapewniać możliwości monitorowania całego systemu i wdrażania w nim konfiguracji VLAN
5. Musi udostępniać narzędzia automatycznej identyfikacji urządzeń instalowanych w sieci

6. Musi zapewniać kompleksowe wsparcie zdalnego zarządzania dla wszystkich proponowanych urządzeń sieciowych, jak również wszystkich urządzeń zarządzanych przez SNMP MIB-I oraz MIB-II
7. Do obsługi zdalnej nie może wymagać stosowania żadnych klientów użytkowników końcowych lub oprogramowania typu agent
8. Musi umożliwiać śledzenie atrybutów urządzeń zainstalowanych w sieci, takich jak numer seryjny, etykieta zasobu, wersja oprogramowania firmware, typ CPU i pamięć
9. Musi udostępniać narzędzia graficznej prezentacji urządzeń sieciowych wraz z dynamiczną prezentacją zmiany stanu urządzenia
10. Musi mieć możliwość lokacji systemów końcowych podłączonych do sieci bezprzewodowej WLAN opartej o triangulację z podglądem przemieszczania się terminala w czasie
11. Musi mieć możliwość dodawanie własnych planów pięter, wyświetlanie symulacji pokrycia zasięgiem sieci bezprzewodowej z możliwością podglądu wykorzystanych kanałów 802.11

wymagania szczegółowe dla systemu zarządzania siecią zawarto w specyfikacji technicznej projektu wykonawczego dla branży niskoprądowej

5.3.7 System kontroli dostępu – Network Acces Control

System kontroli dostępu musi umożliwiać objęcie swoim działaniem wszystkich urządzeń (LAN/WLAN) dostarczanych w ramach postępowania. Musi posiadać wsparcie producenta w zakresie pomocy technicznej 24x7x365 oraz aktualizacji oprogramowania na okres 36 miesięcy. Dodatkowo dostęp do bazy wiedzy producenta, która zapewnia bezpośredni dostęp np. do dokumentacji.
Jeżeli w oferowanym systemie licencje są czasowe, ograniczające w jakikolwiek sposób funkcjonalność rozwiązania, Zamawiający wymaga dostarczenia licencji na okres nie mniejszy niż 10 lat.

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

wymagania szczegółowe dla systemu kontroli dostępu sieciowego zawarto w specyfikacji technicznej projektu wykonawczego dla branży niskoprądowej

5.3.8 Wymagania realizacyjne i gwarancyjne

- Wykonawca musi być autoryzowanym partnerem producenta oferowanych rozwiązań, mogącym świadczyć serwis oparty na świadczeniach producenta - do oferty należy załączyć dokument potwierdzający autoryzacje (certyfikat lub pisemne potwierdzenie producenta lub jego polskiego przedstawicielstwa);
- Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów – do oferty należy dołączyć odpowiednie oświadczenie Wykonawcy;
- Zamawiający wymaga, by dostarczone urządzenia były nowe oraz nieużywane;
- Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne w okresie wymaganym w SIWZ – do oferty należy dostarczyć odpowiednie oświadczenia Wykonawcy;
- Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień poprzedzający dzień składania ofert;

Wymagania na usługi w ramach realizacji instalacji:

Lp	Nazwa wymagana	Wymagania minimalne:
1	Gwarancja podstawowa na urządzenia aktywne	Wymagane jest, aby urządzenia aktywne posiadały min. 60-cio miesięczną gwarancję producenta z zachowaniem poniższych warunków: a. bezpłatne aktualizacje firmware b. wysyłkę uszkodzonego komponentu z wysyłką następnego dnia roboczego od uznania awarii c. dostęp do bazy wiedzy producenta
2	Wsparcie dla oprogramowania (Kontroler WLAN, NMS, NAC)	Oprogramowanie musi posiadać wsparcie producenta w zakresie pomocy technicznej 24x7x365 oraz aktualizacji oprogramowania na okres 36 miesięcy. Dodatkowo dostęp do bazy wiedzy producenta, która zapewnia bezpośredni dostęp np. do dokumentacji.
3	Gwarancja na usługę	W cenie dostawy wymagane jest udzielenie min 36 miesięcznej gwarancji na wykonanie usługi instalacji, skonfigurowanie z systemem zarzadzania siecią i poprawne działanie urządzeń aktywnych (switch'y) w sieci.
4	Licencje czasowe	• Jeżeli którekolwiek wymagane funkcje urządzeń są ograniczone licencjami czasowymi, muszą być dostarczone z zapewnieniem funkcjonalności na okres min. 10 lat. • Jeżeli w oferowanym oprogramowaniu którekolwiek licencje są czasowe, ograniczająca w jakikolwiek sposób funkcjonalność rozwiązania, Zamawiający wymaga dostarczenia licencji na okres nie mniejszy niż 10 lat.
5	Montaż i wstępne uruchomienie urządzeń	Dostawa urządzeń, montaż urządzeń w przygotowanych miejscach do sprawnej sieci LAN, wstępne uruchomienie wszystkich elementów systemu, połączenie elementów w jednolity system z wykorzystaniem istniejącego okablowania, podłączenie urządzeń do sieci zasilającej.

6	Instalacja i uruchomienie	Wykonanie instalacji zgodnie z załączonym wykazem, obejmującego minimum: a. Instalację niezbędnego sprzętu, b. Konfigurację switchy: • konfigurację portów przełączników, konfiguracja VLAN, • routing pomiędzy sieciami wirtualnymi, • bezpieczeństwo switchy (zabezpieczenie przełączników), • implementację spanning tree, • backup urządzeń. c. Wykonanie wszystkich niezbędnych połączeń pomiędzy warstwami: corową, oraz dystrybucyjną, a także przyłączenie do infrastruktury sieciowej budynku.
7	Instalacja i konfiguracja oprogramowania	Instalacja i podstawowa konfiguracja oprogramowania: NMS, NAC.
8	Szkolenie - poziom podstawowy	1-dniowe szkolenie dla min. 3 osób w godz. 8-16 w siedzibie Klienta: Program szkolenia – zagadnienia: Konfiguracja podstawowa switchy z poziomu systemu NMS: - Konfiguracja portów przełączników, konfiguracja VLAN - Routing pomiędzy sieciami wirtualnymi - Bezpieczeństwo switchy (zabezpieczenie przełączników) - Implementacja spanning tree - Implementacja redundancji na switchach (stackowanie switchy) - Backup urządzeń Wykonawca wystawi certyfikaty potwierdzające ukończenie szkolenia.
9	Wdrożenie i konfiguracja systemu NMS i NAC	Stworzenie, implementacja i wdrożenie w systemie: - centralnego zarządzania wszystkimi urządzeniami sieciowymi z jednej konsoli, - grup użytkowników i powiązanych z nimi zasobów sieciowych, - powiązanych z użytkownikami polityk bezpieczeństwa, - portalu logowania do autentykacji użytkowników, także gości, - instalacja i konfiguracja serwera RADIUS, - definicji profili NAC i powiązanie ich z politykami bezpieczeństwa, - etapowego uruchomienia systemu NAC (1. etap: NAC w trybie pasywnym z podstawowym dostępem do sieci, 2. etap: włączenie zróżnicowanego dostępu do sieci w oparciu o wyniki autentykacji), - testów funkcjonalnych po każdym etapie wdrożenia i korekty wykrytych nieprawidłowości
10	Szkolenie - poziom zaawansowany	4-dniowe szkolenie dla min. 2 osób w godz. 8-16 w centrum szkoleniowym Producenta (voucher na szkolenie do wykorzystania, ważny 1 rok) Program szkolenia - zagadnienia: - omówienie podstawowych funcjonalności systemu NAC - definiowanie polityk w NMS i profili oraz reguł NAC - Analityka: podstawowe kwestie związane z konfiguracją, wyborem punktów monitorowania ruchu w sieci oraz interpretacja prezentowanych danych
11	Certyfikat potwierdzający partnerstwo Wykonawcy	Wymagane jest posiadanie certyfikatu potwierdzającego partnerstwo Wykonawcy, udzielone przez producenta oferowanego rozwiązania oraz legitymowanie się możliwościami wydelegowania co najmniej jednego inżyniera certyfikowanego przez producenta oferowanego rozwiązania.

5.4 Elementy systemu IP

5.4.1 Parametry techniczno-funkcjonalne dla systemu telefonii IP

1) Wszystkie niżej wymienione elementy i funkcjonalności oferowanego serwera teleinformatycznego muszą pochodzić od jednego producenta, co umożliwi najwyższy stopień integracji funkcjonalnej i technicznej rozwiązania oraz ujednolici zarzadzanie i administrację, w szczególności:
   a. Wszystkie rodzaje telefonów cyfrowych:
      i. pracujące na bazie sieci komputerowej,
      ii. bezprzewodowe pracujące w standardzie:
         1. DECT,
         2. WLAN,
      iii. przystawki i adaptery do telefonów,
   b. System IP-DECT,
   c. Oprogramowanie:
      i. UC,
      ii. multimedialne Contact Center,
      iii. telefonów programowych (softphone):
         1. cyfrowych,
         2. SIP,
      iv. monitoring wideo,
      v. do szyfrowania i tunelowania,
2) Oferowany serwer teleinformatyczny musi zapewniać funkcje charakterystyczne dla klasycznej centrali telefonicznej, takie jak: przekierowanie rozmów (natychmiastowe, z opóźnieniem na zajętości), przyjmowanie połączeń (indywidualne, grupowe), połączenia trójstronne, połączenia brokerskie, zawieszanie rozmów, wybieranie skrócone grupowe i indywidualne, sygnalizacja rozmowy oczekującej, zamawianie oddzwaniania (na zajętości, przy braku odpowiedzi), obsługa oczekujących wiadomości, paging, przechwytywanie rozmów.
3) Oferowany serwer teleinformatyczny musi umożliwiać uruchomienie wewnętrznego serwera Unified Communication (UC) dla co najmniej:
   a. 50 użytkowników z funkcjonalnością standardową, udostępniającą poniższy zakres funkcji:
      i. prowadzenie bazy kontaktów, m.in. numeracji telefonicznej, adresacji, e-mail, itp.,
      ii. wizualizacji informacji o połączeniach: przychodzących, wychodzących, odebranych, nieodebranych,
      iii. ustalanie statusu obecności abonenta (np.: w biurze, na spotkaniu, przerwa, chory, poza biurem, na urlopie, przerwa na lunch, w domu) dla minimum 6 różnych scenariuszy,
      iv. tworzenie własnego menu zapowiedzi słownych stosownie do wybranego statusu prezencji/obecności dla minimum 6 różnych scenariuszy,
      v. wysyłanie krótkich wiadomości tekstowych pośród użytkowników serwera oraz klientami z wykorzystaniem otwartego protokołu XMPP (np. Google Talk),
      vi. integrację statusów prezencji/obecności z komunikatorami Instant Messaging innych producentów (media społecznościowe) za pomocą otwartego protokołu XMPP,
   b. 150 użytkowników z funkcjonalnością zaawansowaną, udostępniającą ponadto poniższy zakres funkcji dodatkowych:
      i. wybieranie zaznaczonych numerów telefonicznych wprost ze stron internetowych lub dokumentów elektronicznych,
      ii. wysyłanie i odbieranie faksów bezpośrednio na/z komputer użytkownika,
      iii. odbieranie faksów na e-mail,
      iv. zarzadzanie zintegrowanym mostkiem konferencyjnym przez www,
      v. nagrywanie rozmów na żądanie.
4) Oprogramowanie klienta UC musi być dostępne jako:
   a. samodzielna aplikacja dla MS Windows i Apple Mac OS X,
   b. dodatek do MS Outlook dla MS Windows i Apple Mac OS X,
   c. wersja mobilna dla pracowników mobilnych z wykorzystaniem smartfonów lub tabletów z graficznym interfejsem użytkownika, takich jak: iPhone, Blackberry, Nokia, Android i Windows Mobile,
   d. aplikacja na wybrane telefony systemowe IP, umożliwiająca użytkownikom dostęp do funkcji poczty głosowej i zarządzanie statusami obecności.
5) Oferowany serwer teleinformatyczny musi umożliwiać korzystanie z Wizualnej Poczty Głosowej zapewniającej:
   a. 300 skrzynek poczty głosowej,
   b. Sterowanie własną skrzynką głosową poprzez interfejs telefoniczny (TUI) lub ekran komputera (GUI) poprzez oprogramowanie klienta UC,

c. Skrzynki grupowe (MWI dla wszystkich członków grupy),
d. Możliwość dograna komentarza do nagranej wiadomości i przesłanie go na skrzynki poczty głosowej jednego lub wielu użytkowników,
e. Wiadomości głosowe mogą być automatycznie przesyłane jako e-maile do konkretnych użytkowników.

6) Oferowany serwer teleinformatyczny musi umożliwiać korzystanie z 2 rodzajów konferencji:
a. Konferencje standardowe:
   i. 6 konferencji po 5 użytkowników,
   ii. zarządzanie konferencją z telefonów systemowych (TUI),
   iii. przeglądanie listy uczestników danej konferencji z możliwością ich selektywnego odłączania lub dołączania.
b. Konferencje zaawansowane dostępne poprzez oprogramowanie klienta UC:
   i. Maksymalnie 16 użytkowników w jednej konferencji,
   ii. Wdzwaniane – na udostępniony numer pokoju konferencyjnego,
   iii. Wydzwaniane - uczestnicy są wydzwaniani przez organizatora konferencji,
   iv. Konferencje stałe (zaplanowane, powtarzane cyklicznie lub jednorazowe),
   v. Konferencje z wymaganą autoryzacja poprzez PIN-kod lub bez weryfikacji,
   vi. Konferencje otwarte – z możliwością zdefiniowania maksymalnej ilości uczestników,
   vii. ręczne lub automatyczne wysyłanie powiadomień o planowanej konferencji (zaproszeń),
   viii. automatyczny wpis o przyszłej konferencji do kalendarzy MS Outlook uczestników konferencji,
   ix. zwoływanie konferencji ad-hoc poprzez:
      1. przeciągnięcie na ekran ikon użytkowników, których udział planowany jest w konferencji,
      2. dobranie dowolnych użytkowników poprzez wpisanie ich numerów i nazw,
      3. zawieszanie lub odłączenie niepotrzebnych użytkowników konferencji,
   x. graficzny podgląd konferencji na ekranie komputera z pełną informacją graficzną o statusie obecności oraz fazie połączenia (dzwoni telefon, podniósł słuchawkę, rozłączył się) uczestników konferencji,
   xi. możliwość rozszerzenia konferencji o pracę grupową (oprogramowanie do pracy grupowej) poprzez jedno kliknięcie na ekranie,
   xii. możliwość ustawienia nagrywania konferencji a następnie otrzymania jej treści poprzez wizualną pocztę głosową.

7) Oferowany serwer teleinformatyczny musi umożliwiać nagrywanie rozmów wewnętrznych i zewnętrznych (zintegrowany rejestrator rozmów) dla wszystkich użytkowników, wyposażonych w oprogramowanie klienta UC w wersji zaawansowanej. Zintegrowany rejestrator rozmów umożliwia:
a. Nagrywanie na żądanie – dla każdego wyżej opisanego użytkownika,
b. Nagrywanie permanentne – dla wszystkich konferencji zaawansowanych,
c. Zarządzanie nagraniami poprzez wizualną pocztę głosową z wykorzystaniem jej pełnej funkcjonalności.

8) Oferowany serwer teleinformatyczny musi udostępniać wewnętrzną (integralny element serwera w wykonaniu sprzętowym) bramę VoIP:
a. udostępniającą minimum 8 kanałów uniwersalnych głosowych,
b. umożliwiającą rozbudowę 128 kanałów VoIP,
c. pozwalającą podłączonym terminalom na komunikację bezpośrednią (bez zajmowania kanałów głosowych) bez ograniczeń co do funkcjonalności tych urządzeń.

9) Wewnętrzny system zapowiedzi słownych musi zapewniać:
a. wielopoziomowe powitanie firmowe z przekierowaniem do wybranego abonenta, do grupy, na pocztę głosową,
b. w przypadku wykorzystania oprogramowania UC – dostosowanie zapowiedzi w języka dzwoniącego (w zakresie wgranych do systemu języków, rozpoznawanie poprzez numer kierunkowy kraju dzwoniącego).

10) Oferowany serwer teleinformatyczny musi udostępniać wewnętrzny serwer faksowy umożliwiający:
a. skonfigurowanie maksymalnie skrzynek faksowych z własnymi numerami, ilu jest użytkowników,
b. wysyłanie i odbieranie faksów bezpośrednio z/na osobisty komputer współpracujący z aparatem telefonicznym,
c. odbieranie faksów na e-mail,
d. wydrukowanie faksu, zapisanie w na dysku komputera lokalnego, przesłanie faksu do wybranych użytkowników,
e. sterowanie własną skrzynką faksową poprzez oprogramowanie klienta UC (GUI),
f. zapewnienie bezpieczeństwa przechowywanych faksów i dostęp do nich w każdej chwili.

11) Oferowany serwer teleinformatyczny musi udostępniać poniższe funkcje związane z mobilnością (Klient Mobilny):
a. Dostępność na smartfon/tablet oprogramowania klienta UC,
b. Usługę Jednego Numeru – dla klientów udostępniany jest 1 numer (stacjonarny) użytkownika, pod którym jest on osiągalny dla osób dzwoniących do niego. W zależności od statusów obecności

następuje przekierowanie rozmowy przychodzącej na właściwe urządzenie końcowe. Poza tym serwer udostępnia numer do wdzwaniania dla użytkowników mobilnych, po dodzwonieniu się udostępnia im własne konto telefoniczne i wszystkie usługi z nim związane.

c. Usługę Dzwoń Do Mnie – funkcja oddzwaniania przez system, gdy użytkownik jest poza biurem. Chcąc połączyć się z klientem użytkownik mobilny wybiera jego numer z oprogramowania klienta UC, serwer zestawia na swój koszt połączenie do użytkownika mobilnego a następnie zestawia połączenie do klienta.

Jeśli klient zadzwoni do użytkownika mobilnego na jego numer - serwer zestawi połączenie na wskazany numer zewnętrzny; urządzenie mobilne, telefon stacjonarny w domu lub hotelu,

d. Widoczność stanów połączeniowych użytkowników mobilnych dla innych użytkowników UC – stany: zalogowany telefonem mobilnym, jego telefon dzwoni, rozmawia, nie przeszkadzać,

e. Usługę „Wspólne Biurko" - umożliwia wielu użytkownikom korzystanie z jednego telefonu. Każdy użytkownik będąc w biurze loguje się na telefonie swoim kodem PIN, który umożliwia mu dostęp do osobistych ustawień telefonu.

12) Oferowany serwer teleinformatyczny musi udostępniać:

a. narzędzie do integracji z aplikacjami biznesowymi Zamawiającego:

i. Elastyczność - przekazywanie 5 kryteriów (identyfikatorów klienta) do aplikacji Zamawiającego, dobieranych odpowiednio do potrzeb,

ii. Uruchomienie aplikacji Zamawiającego w oparciu o:

1. wykonanie pliku wsadowego,
2. URL (np. książki telefoniczne online lub lokalizacja poprzez Google Maps),
3. elastyczne wyskakujące okienka z konfigurowalnymi przyciskami akcji umożliwiające wykonywanie określonych aplikacji na żądanie,

b. integrację z aplikacjami komputerowymi CTI w oparciu o standardy: Microsoft TAPI 2.1, Microsoft TAPI 3.0, CSTA phase I, CSTA phase III, CSTA III XML,

c. protokół CSTA phase III zgodny z normą ECMA 385. Protokół dostępny na styku ISDN oraz LAN. Ilość monitorowanych obiektów – min.100.

13) Oferowany serwer teleinformatyczny musi udostępniać wbudowane narzędzie do integracji z bazami danych Zamawiającego:

b. dostęp do wszystkich katalogów oferowanego serwera teleinformatycznego z aplikacji 3rd party,

c. podłączenie do co najmniej niżej wymienionych zewnętrznych baz danych:

i. PostgreSQL,
ii. Microsoft SQL Server 2000 / 2005 / 2008,
iii. Sybase SQL Server V10 i późniejsze.

d. łączenie wewnętrznych katalogów oferowanego serwera teleinformatycznego i zewnętrznych baz danych w jeden ujednolicony interfejs użytkownika w wyszukiwarkach,

e. zarządzanie i konfiguracja za pośrednictwem okien zarzadzania serwera teleinformatycznego.

14) Oferowany serwer teleinformatyczny musi umożliwiać budowę Multimedialnego Contact Center zapewniającego co najmniej:

a. korzystanie z możliwości oprogramowania UC (pełna integracja z możliwością korzystania z narzędzi do integracji z aplikacjami biznesowymi oraz bazami danych Zamawiającego włącznie),

b. jednoczesną pracę min. 60 agentów,

c. obsługę wielu kanałów komunikacji:

i. rozmowa telefoniczna, poczta głosowa,
ii. e-mail,
iii. faks,

d. indywidualne komunikaty w przypadku wydłużającego się czasu oczekiwania w kolejce w tym możliwość przekierowania do innej kolejki oraz pozostawienia wiadomości na którą odpowie wolny agent,

e. przypisanie agentów do wielu grup w których mogą mieć różne umiejętności na różnym poziomie. Contact Center zapewni połączenie z pierwszym wolnym agentem o odpowiednich kompetencjach (Skill Based Routing),

f. preferowany agent - możliwość takiego skonfigurowania Contact Center, aby połączenia od poszczególnych klientów przekazywane były zawsze do przydzielonych im osób kontaktowych,

g. obsługa klientów VIP - możliwość bezpośredniego przekierowywania klientów VIP do wolnych agentów, bez konieczności oczekiwania w kolejce na połączenie,

h. wskazówki głosowe zależne od numeru - odtwarzanie indywidualnych komunikatów w reakcji na numer telefonu rozmówcy w jego ojczystym języku,

i. czas na podsumowanie połączenia – po każdej rozmowie można ustawić czas przerwy, w czasie której agent będzie mógł np. uzupełnić formularz kontaktu.

j. zróżnicowane poziomy uprawnień dla użytkowników Contact Center,

k. szczegółowa lista dzwoniących - informacje na temat wszystkich połączeń, faksów i wiadomości e-mail, które do chwili obecnej znajdują się w liście dzwoniących do Contact Center.

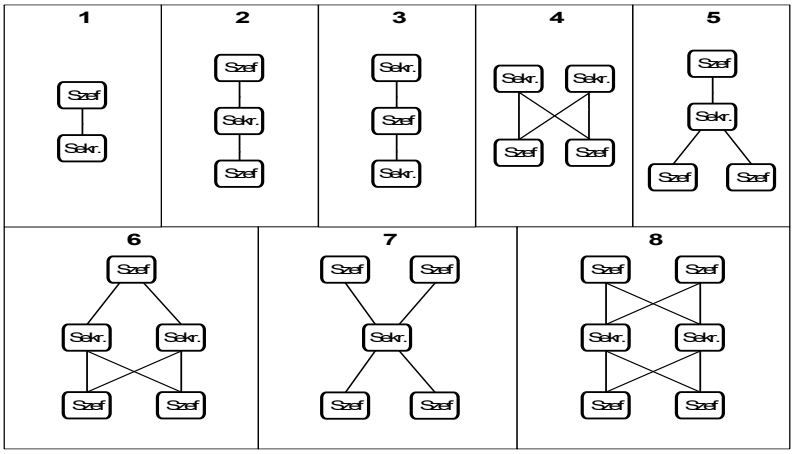
l. Aplikacja Agenta Contact Center (element oprogramowania UC) musi umożliwiać:
   i. szybką konsultację agentów z innymi specjalistami dzięki zintegrowanej funkcji wyświetlania obecności, ponieważ agent może w każdej chwili sprawdzić, który specjalista jest wolny i może udzielić mu pomocy,
   ii. ciągłe sprawdzanie, ilu dzwoniących wciąż oczekuje w kolejce i odpowiedniego reagowania na sytuację,
   iii. wygenerowanie ponad 20 zdefiniowanych raportów, wykazujących np. ile połączeń odebrał agent,

m. Aplikacja Raporty – musi umożliwiać:
   i. generowanie danych statystycznych dotyczących korzystania z Contact Center, posortowanych według różnych kryteriów,
   ii. dostępność min. 100 innych wzorów raportów,
   iii. indywidualne generowanie i dostosowywanie raportów.

15) Oferowany serwer teleinformatyczny musi umożliwiać budowanie zaawansowanych układów sekretarsko – dyrektorskich. Elastyczna konfiguracja musi pozwalać na budowę poniższych układów z zastosowaniem do 4 aparatów dyrektorskich i do 2 aparatów sekretarskich. Układ musi realizować następujące funkcje:

a.„przełączenie dzwonienia do szefa ” służący do aktywacji lub dezaktywacji funkcji buforowania rozmów do szefa przez sekretariat,
b. „połączenie bezpośrednie –” do każdego szefa,
c.„połączenie bezpośrednie –” do każdej sekretarki,
d. „przejęcie rozmowy ”,
e.„zastępstwo”,

Dostępne są poniższe aranżacje układu sekretarsko-dyrektorskiego bez konieczności zakupu dodatkowych licencji:



16) Oferowany serwer teleinformatyczny musi umożliwiać uruchomienie oprogramowania do pracy grupowej, które udostępni:
   f. szyfrowanie transmisji kluczem 256 bitów (najwyższe bezpieczeństwo),
   g. udostępnianie innym członkom grupy wybranych elementów własnego ekranu,
   h. wirtualne repozytorium plików, do i z którego każdy członek grupy może w ramach sesji przesyłać i pobierać pliki,
   i. funkcję softphone (komunikacja głosowa w ramach sesji przez komputer),
   j. wideokonferencje – przesyłanie do 8 strumieni wideo jakości HD zakodowanych za pomocą protokołu H.264,
   k. możliwość dołączania klientów zewnętrznych nie związanych z oferowanym serwerem teleinformatycznym,
   l. max. 250 uczestników, max. 30 jednoczesnych transmisji głosowych, pozostali uczestniczą w roli słuchaczy.
17) Oferowany serwer teleinformatyczny musi umożliwiać podłączenie oprogramowania dla stanowiska Awizo / Asystent do obsługi i zarządzania połączeniami, współpracującą z serwerem UC, umożliwiającą wizualną prezentację statusu/obecności użytkowników, zarządzanie skrzynkami pocztowymi, faksowymi i statusami użytkowników, którzy wyrazili na to zgodę, wysyłanie widomości błyskawicznych do użytkowników.
18) Architektura oferowanego serwera teleinformatycznego i możliwości jego rozbudowy:
   a. wsparcie dla wirtualizacji VMware vSphere i Microsoft Hyper-V,
   b. umożliwia uruchomienie 500 abonentów IP,
   c. pojemność serwera teleinformatycznego w wersji wielomodułowej to 1000 abonentów IP w tym do 300 abonentów IP-DECT,
19) Musi umożliwiać instalację w chmurze prywatnej i umożliwia instalację oprogramowania klienta UC dla MS Outlook w oprogramowaniu MS Office 365 (również w chmurze).

20) Oferowany serwer teleinformatyczny musi posiadać zdolność do sieciowania z innymi serwerami teleinformatycznymi tego samego producenta z wykorzystaniem połączeń typu VoIP - tunelowanych i szyfrowanych (wersja programowa),
21) Sieciowanie musi umożliwiać pełną wymianę usług i funkcjonalności z wykorzystaniem obecnie stosowanych przez producenta tych serwerów protokołów.
22) Oferowany serwer teleinformatyczny musi umożliwiać sieciowanie wielu modułów i zarzadzanie nimi jak jednym urządzeniem (rozproszony serwer stakowalny). Serwer w wykonaniu wielomodułowym z oprogramowaniem UC umożliwia realizację poniższych cech / funkcjonalności dla dowolnych abonentów dowolnych zsieciowanych modułów:
    a. Głos wspierany zarządzaniem obecnością (podgląd statusów obecności),
    b. Status połączenia w całej sieci (dzwonienie, trwa rozmowa, aktywne urządzenie mobilne),
    c. Odbieranie połączeń za pośrednictwem programu klienckiego UC,
    d. Komunikator w tym czat wielu użytkowników jednocześnie,
    e. Konferencje zaawansowane,
    f. Współpraca w sieci (ze współdzieleniem pulpitów i wideo),
    g. Przekierowanie poczty głosowej w sieci,
    h. Oprogramowania dla stanowisk awizo ma możliwość zmiany statusów obecności dla wszystkich użytkowników,
    i. Spis numerów wewnętrznych całego systemu oraz indywidualne listy ulubionych kontaktów poszczególnych użytkowników („Ulubione”),
    j. Katalogi zewnętrzne za pośrednictwem narzędzia do integracji z bazami danych,
    k. Integracja z kalendarzem MS Exchange i folderami publicznymi,
    l. Oparte na XMPP wsparcie obecności i czatu do partnerów zewnętrznych (kontrahentów),
    m. Informacja o zajętości w całej sieci na lampkach przy klawiszach DSS w telefonach systemowych.
23) Oferowany serwer teleinformatyczny musi umożliwiać uruchomienie oprogramowania sterującego IP-DECT bez konieczności instalacji opcjonalnego zewnętrznego serwera IP-DECT dla:
    a. max. 10 stacji bazowych IP-DECT,
    b. max. 50 telefonów bezprzewodowych DECT,
24) Oferowany serwer teleinformatyczny musi opcjonalnie udostępniać telefony bezprzewodowe DECT realizujące odpowiednio poniższe wymagania:
    a. przeznaczone do pracy biurowej,
    b. o wysokiej wytrzymałości - spełniające wymagania ochrony IP65,
    c. iskrobezpieczne – certyfikowane do pracy w środowiskach z atmosferą zagrażającą wybuchem.
25) Oferowany serwer teleinformatyczny musi umożliwiać uruchomienie opcjonalnego wewnętrznego systemu monitoringu wideo min. 2 kamer CCTV, z których obraz transmitowany będzie na max. 10 urządzeń odbiorczych w tym:
    a. Ekrany telefonów systemowych zaawansowanych IP,
    b. Ekrany telefonów iPhone,
    c. Ekrany komputerów z zainstalowanym klientem systemu monitoringu wideo.
26) Oferowany serwer teleinformatyczny musi umożliwiać podłączenie aplikacji współpracującej z oprogramowaniem zarządzającym (patrz: Zgodność z wymaganiami KRI), zapewniającej działanie następujących funkcjonalności:
    a. zintegrowane zarządzanie urządzeniami IP i bezpieczeństwem,
    b. centralne zarządzanie wersjami oprogramowania telefonów IP (np. zarzadzanie konfiguracją i aktualizacje oprogramowania),
    c. zapewnienie dla użytkowników końcowych automatycznej transmisji wszystkich parametrów wymaganych przez urządzenie w momencie pierwszego podłączenia do sieci (funkcja Plug&Play),
    d. zachowanie wszystkich ustawień osobistych użytkownika (tj. układ klawiszy, książka telefoniczna, listy połączeń, tony dzwonka, wygaszacz ekranu) i udostępnienie ich w momencie, gdy użytkownik loguje się do dowolnego telefonu**.**

5.4.2 Parametry techniczno-funkcjonalne dla urządzeń

Wymagania minimalne dla cyfrowych aparatów telefonicznych IP:

Aparat telefoniczny systemowy prosty IP musi posiadać:

- możliwość automatycznego upgradu oprogramowania z poziomu centralnego serwera służącego do aktualizacji oprogramowania,
- dwuliniowy wyświetlacz,

- możliwość rozmowy w trybie głośnomówiącym (w trybie full-duplex),
- możliwość rozbudowy o przystawkę z przyciskami funkcyjnymi,
- przyciski do swobodnego programowania funkcji / numeracji, regulacji głośności itp.
- zdolność zarządzania poprzez przeglądarkę WWW,
- zdolność zasilania poprzez port switch-a POE (Power over Ethernet)
- zdolność do obsługi kodeków G.711, G.722, G.729AB,
- możliwość zmiany oprogramowania aparatu na wersję SIP,
- wbudowany własny switch do podłączenia komputera PC pracującego w innej podsieci VLAN niż telefon,

Aparat telefoniczny systemowy sekretarski IP G musi posiadać:

- możliwość automatycznego upgradu oprogramowania z poziomu centralnego serwera służącego do aktualizacji oprogramowania,
- co najmniej czteroliniowy wyświetlacz,
- możliwość podłączenia nagłownego zestawu słuchawkowego,
- możliwość rozbudowy o przystawkę z przyciskami funkcyjnymi,
- możliwość rozmowy w trybie głośnomówiącym (w trybie full-duplex),
- przyciski do swobodnego programowania funkcji / numeracji, regulacji głośności itp.
- zdolność zarządzania poprzez przeglądarkę WWW,
- zdolność zasilania poprzez port switch-a POE (Power over Ethernet),
- zdolność do obsługi kodeków G.711, G.722, G.729AB,
- możliwość zmiany oprogramowania aparatu na wersję SIP,
- wbudowany własny switch 10/100/1000 Mbps do podłączenia komputera PC pracującego w innej podsieci VLAN niż telefon,
-

Aparat telefoniczny systemowy zaawansowany IP VIP musi posiadać:

- możliwość automatycznego upgradu oprogramowania z poziomu centralnego serwera służącego do aktualizacji oprogramowania,
- wyświetlacz kolorowy o przekątnej min. 4 cale i rozdzielczości min. QVGA,
- gniazdo USB,
- min. 8 klawiszy programowalnych jako klawisze pamięci lub funkcje
- min. 4 klawisze kontekstowe których znaczenie zmienia się w zależności od stanu telefonu,
- możliwość prowadzenia rozmów wideo po podłączeniu dodatkowej zewnętrznej kamery USB,
- możliwość podłączenia nagłownego zestawu słuchawkowego
- możliwość rozbudowy o przystawkę z przyciskami funkcyjnymi
- możliwość rozmowy w trybie głośnomówiącym (w trybie full-duplex)
- przyciski do swobodnego programowania funkcji / numeracji, regulacji głośności itp.
- Prezentacja zdjęcia kontaktu na wyświetlaczu telefonu systemowego,
- zdolność zarządzania poprzez przeglądarkę WWW,
- zdolność zasilania poprzez port switch-a POE (Power over Ethernet),
- zdolność do obsługi kodeków G.711, G.722,G.729AB,
- możliwość zmiany oprogramowania aparatu na wersję SIP,
- wbudowany własny switch 10/100/1000 Mbps do podłączenia komputera PC pracującego w innej podsieci VLAN niż telefon,

Aparat telefoniczny systemowy IP zaawansowany Contact Center musi posiadać:

- możliwość automatycznego upgradu oprogramowania z poziomu centralnego serwera służącego do aktualizacji oprogramowania,
- wyświetlacz kolorowy o przekątnej min. 4 cale,
- gniazdo USB,
- wbudowany bluetooth,
- możliwość podłączenia nagłownego zestawu słuchawkowego
- możliwość rozbudowy o przystawkę z przyciskami funkcyjnymi
- możliwość rozmowy w trybie głośnomówiącym (w trybie full-duplex)
- przyciski do swobodnego programowania funkcji / numeracji, regulacji głośności itp.
- Prezentacja zdjęcia kontaktu na wyświetlaczu telefonu systemowego
- zdolność zarządzania poprzez przeglądarkę WWW,
- zdolność zasilania poprzez port switch-a POE (Power over Ethernet),
- zdolność do obsługi kodeków G.711, G.722,G.729AB,
- możliwość zmiany oprogramowania aparatu na wersję SIP,
- wbudowany własny switch 10/100/1000 Mbps do podłączenia komputera PC pracującego w innej podsieci VLAN niż telefon,
- możliwość wgrania oprogramowania do prezentacji statusów w rozumieniu oprogramowania UC, wybranych abonentów serwerów telekomunikacyjnych IP, na wyświetlaczu telefonu.

Softphone systemowy musi umożliwiać:

- uruchomienie w wersji paska narzędziowego przytwierdzonego do góry ekranu, zajmującego niewiele miejsca,
- elementy interfejsu jask np. klawiatura, klawisze funkcyjne mogą zostać umieszczone w dowolnej części ekranu,
- funkcjonalność telefonu systemowego z wyświetlaczem i przyciskami programowalnymi z podglądem innych abonentów serwera teleinformatycznego,
- dostęp do usług katalogowych,
- historia połączeń,
- dostęp do funkcjonalności serwera teleinformatycznego,
- modularny interfejs użytkownika umożliwiający zbudowanie indywidualnego układu okien, każde z oddzielnymi modułami funkcjonalnymi.

Softphone SIP musi umożliwiać:

- uruchomienie w wersji paska narzędziowego przytwierdzonego do góry ekranu, zajmującego niewiele miejsca,
- elementy interfejsu jask np. klawiatura, klawisze funkcyjne mogą zostać umieszczone w dowolnej części ekranu,
- realizacja połączeń wideo z sygnalizacja H. 263,
- funkcjonalność telefonu SIP z wyświetlaczem i przyciskami programowalnymi,
- dostęp do usług katalogowych,
- historia połączeń,
- modularny interfejs użytkownika umożliwiający zbudowanie indywidualnego układu okien, każde z oddzielnymi modułami funkcjonalnymi.

Wymagania minimalne dla cyfrowych bezprzewodowych aparatów telefonicznych DECT:

1. Telefon bezprzewodowy DECT biurowy standardowy:
   - Dostęp do funkcji systemowych serwera,
   - Korzystanie z połączenia Bluetooth

- Własna książka telefoniczna na minimum 500 wpisów,
- Własna historia połączeń dla minimum 30 nieodebranych rozmów

2. Telefon bezprzewodowy DECT biurowy VIP:
   - Jak wyżej oraz alarm wibracyjny

3. Telefon bezprzewodowy DECT przemysłowy:
   - Jak wyżej oraz zapewnia zwiększoną odporność konieczną do pracy w warunkach przemysłowych.

Wymagania minimalne dla zewnętrznego systemu rejestracji rozmów SIP-Trunk

1) Wymagana jest wersja programowa rejestratora instalowana na klastrze wysokiej dostępności.
2) Ciągła rejestracja 30 kanałów głosowych SIP-Trunk.
3) Dostęp do rozmów VoIP w celu ich rejestracji realizowany za pomocą monitorowania interfejsu sieciowego.
4) Narzędzia programowe do filtrowania rekordów oraz ustalania czarnej i białej listy

Wymagania minimalne dla oprogramowania taryfikacyjnego

1) System musi być systemem kompleksowego rozwiązania zapewniającego rejestrację, taryfikację oraz wizualizację danych dotyczących zrealizowanych połączeń telefonicznych;
2) Wdrożony system musi umożliwi zbieranie rekordów CDR oraz przetwarzanie danych taryfikacyjnych w zakresie rejestrowania połączeń wychodzących i przychodzących;
3) Sposób taryfikacji odpowiadał będzie rzeczywistym planom taryfowym i prowadzony będzie w oparciu o taryfy przypisane do SIP-Trunka;
4) Raportowanie danych realizowane będzie z wykorzystaniem predefiniowanych raportów w systemie bilingowym.
5) System zostanie zainstalowany w systemie klastra wysokiej dostępności.
6) Minimalna ilość taryfikowanych użytkowników – 300.

5.4.3 Wymagania realizacyjne i gwarancyjne

Lp	Nazwa wymagana	Wymagania minimalne:
1	Gwarancja na urządzenia	Wymagane jest, aby urządzenia posiadały min. 36-cio miesięczną gwarancję.
2	Wsparcie dla oprogramowania	Oprogramowanie musi posiadać wsparcie producenta w zakresie pomocy technicznej 24x7x365 oraz dostęp do aktualizacji oprogramowania na okres 36 miesięcy. Dodatkowo dostęp do bazy wiedzy producenta, która zapewnia bezpośredni dostęp np. do dokumentacji.
3	Licencje czasowe	• Jeżeli którekolwiek wymagane funkcje urządzeń są ograniczone licencjami czasowymi, muszą być dostarczone z zapewnieniem funkcjonalności na okres min. 10 lat. • Jeżeli w oferowanym oprogramowaniu którekolwiek licencje są czasowe, ograniczająca w jakikolwiek sposób funkcjonalność rozwiązania, Zamawiający wymaga dostarczenia licencji na okres nie mniejszy niż 10 lat.

4	Montaż i wstępne uruchomienie urządzeń	Dostawa urządzeń, montaż urządzeń w przygotowanych miejscach do sprawnej sieci LAN, wstępne uruchomienie wszystkich elementów systemu, połączenie elementów w jednolity system z wykorzystaniem istniejącego okablowania, podłączenie urządzeń do sieci zasilającej.
5	Instalacja i konfiguracja systemu telefonicznego	Konsultacje dotyczące konfiguracji systemu telefonicznego, montaż systemu w stojaku, uruchomienie telefonów systemowych, uruchomienie aplikacji, ustalenie sposobu pracy i wdrożenie systemu Call Center, instalacja oraz konfiguracja systemu taryfikacji, instalacja i uruchomienie systemu rejestracji rozmów
6	Integracja z systemem zarządzania siecią LAN	Po uruchomieniu integracji System zarządzania siecią (NMS) wraz z System kontroli dostępu (NAC) przy współpracy z oferowanym serwerem teleinformatycznym musi zapewnić realizację funkcjonalności zgodnie z wykazem w dziale „ Zgodność z wymaganiami KRI”.
7	Szkolenie - poziom podstawowy	1-dniowe szkolenie dla 3 osób w godz. 8-16 w siedzibie Klienta: Program szkolenia – zagadnienia: szkolenie podstawowe w zakresie wszystkich zainstalowanych komponentów systemu
8	Certyfikat potwierdzający partnerstwo Wykonawcy	Wymagane jest posiadanie certyfikatu potwierdzającego partnerstwo Wykonawcy, udzielone przez producenta oferowanego rozwiązania oraz legitymowanie się możliwościami wydelegowania co najmniej jednego inżyniera certyfikowanego przez producenta oferowanego rozwiązania.

5.5 Zestawienie materiałów

Elementy pasywne

Ilość	Jednostka	Nazwa
Budynek Astronomów		
Gniazda PEL Astronomów (poziom -1 do 2)		
122	szt.	Mounting Plate 45x45 mm, angled, white
187	szt.	Module RJ45/s C6A ISO
130	szt.	Hinged Coloured Dust Cover-green
57	szt.	Hinged Coloured Dust Cover-red
187	szt.	Patch Cord CU PA C6A S GY 3m
260	szt.	Easy Latch-green
114	szt.	Easy Latch-red
Gniazda Floorboxy Astronomów (poziom -1 do 2)		
74	szt.	Mounting Plate 45x45 mm,2 port, flat-white
111	szt.	Module RJ45/s C6A ISO
74	szt.	Hinged Coloured Dust Cover-green
37	szt.	Hinged Coloured Dust Cover-red
111	szt.	Patch Cord CU PA C6A S GY 3m
148	szt.	Easy Latch-green

74	szt.	Easy Latch-red
Gniazda PEL Astronomów (poziom 3 do 4) Izba Wyższa Urzędu		
93	szt.	Mounting Plate 45x45 mm, angled, white
142	szt.	Module RJ45/s C6A ISO
98	szt.	Hinged Coloured Dust Cover-green
44	szt.	Hinged Coloured Dust Cover-red
142	szt.	Patch Cord CU PA C6A S GY 3m
196	szt.	Easy Latch-green
88	szt.	Easy Latch-red
Gniazda Floorboxy Astronomów (poziom 3 do 4) Izba Wyższa Urzędu		
31	szt.	Mounting Plate 45x45 mm,2 port, flat-white
48	szt.	Module RJ45/s C6A ISO
34	szt.	Hinged Coloured Dust Cover-green
14	szt.	Hinged Coloured Dust Cover-red
48	szt.	Patch Cord CU PA C6A S GY 3m
68	szt.	Easy Latch-green
28	szt.	Easy Latch-red
Szafy serwerownia		
2	szt.	Szafa serwerowa 19" 42U 800x1000 RAL 7035 standardowa
2	szt.	KPL.NAROŻNIKÓW COKOŁU 100
4	szt.	ŁĄCZNIK NAROŻNIKÓW PEŁNY /L- 600/ dł. ściany cokołu 800
4	szt.	ŁĄCZNIK NAROŻNIKÓW PEŁNY (L-800) dł. ściany cokołu 1000
2	szt.	Panel wentylacyjny z termostatem, RAL 7035
2	szt.	Zaślepka z włókniną i przepustem szczotkowym RAL 7035
8	szt.	Uchwyt kablowy 88x88 mm (komplet 5 szt.)
8	szt.	Łącznik do szaf serwerowych
6	szt.	Listwa zasilająca z 5 gniazdami 2P+Z z filtrem sieciowym 30MHz
2	szt.	Półka regulowana 1U, gł. 500-900, RAL 7035
1	szt.	Przełącznica 1U-UniRack2-IR-12-lcdzpcBm-om3-dinvde
1	szt.	Przełacznica 1U-UniRack2-IR-6-lcdzpcBm-om3-dinvde
3	szt.	Splice holder 12 x heat shrink protect.
36	szt.	FO Splice protection
2	szt.	FO Cable Guide 75mm for 19"1U Rack
18	szt.	Patch cord FO OM3 LCD/LCD 5m
36	szt.	Plug Guard for LCd connector
4	szt.	Patch panel HD-19" 1U-24xRJ45-C6A ISO/s-
9	szt.	Patch Panel HD-19" 1U-24xRJ45-C6A ISO/s-
32	szt.	CM 1U 19" Metal Panel, Modular 70mm
204	szt.	HDS Level 1-HDC-green
94	szt.	HDS Level 1-HDC-red
297	szt.	Patch Cord CU PA C6A S GY 5m
408	szt.	Easy Latch-green
188	szt.	Easy Latch-red
Szafa PPD (Izba Wyższa Urzędu)		
2	szt.	Szafa serwerowa 19" 42U 800x1000 RAL 7035 standardowa
2	szt.	KPL.NAROŻNIKÓW COKOŁU 100
4	szt.	ŁĄCZNIK NAROŻNIKÓW PEŁNY /L- 600/ dł. ściany cokołu 800
4	szt.	ŁĄCZNIK NAROŻNIKÓW PEŁNY (L-800) dł. ściany cokołu 1000
2	szt.	Panel wentylacyjny z termostatem, RAL 7035
2	szt.	Zaślepka z włókniną i przepustem szczotkowym RAL 7035
8	szt.	Uchwyt kablowy 88x88 mm (komplet 5 szt.)
2	szt.	Półka regulowana 1U, gł. 500-900, RAL 7035
5	szt.	Listwa zasilająca z 5 gniazdami 2P+Z z filtrem sieciowym 30MHz

1	szt.	Przełącznica 1U-UniRack2-IR-6-lcdzpcBm-om3-dinvde
1	szt.	Splice holder 12 x heat shrink protect.
12	szt.	FO Splice protection
1	szt.	FO Cable Guide 75mm for 19"1U Rack
6	szt.	Patch cord FO OM3 LCD/LCD 5m
12	szt.	Plug Guard for LCd connector
3	szt.	PP HD-19" 1U-24xRJ45-C6A ISO/s-
6	szt.	PP HD-19" 1U-24xRJ45-C6A ISO/s-
9	szt.	CM 1U 19" Metal Panel, Modular 70mm
132	szt.	HDS Level 1-HDC-green
58	szt.	HDS Level 1-HDC-red
190	szt.	Patch Cord CU PA C6A S GY 5m
264	szt.	Easy Latch-green
116	szt.	Easy Latch-red
Kable		
27	km	S/FTP 4x2x0,5 4P 650 MHz LSZH
0,05	km	LT-cable-indoor-12-om3
Połączenia pomiędzy budynkami		
2	szt.	Skrzynia zapasu kabla 610/610/100 zamykana na klucz
2	szt.	Przełącznica NS-4 48xSC PC OM3 M/4 Z, wyposażona
48	szt.	Patch cord FO OM3 LCD/LCD 1m
96	szt.	Plug Guard for lcd connector
0,15	km	LT-cable-outdoor-24-om3
Budynek Ciołka		
Gniazda PEL Ciołka		
185	szt.	Mounting Plate 45x45 mm, angled, white
283	szt.	Module RJ45/s C6A ISO
196	szt.	Hinged Coloured Dust Cover-green
87	szt.	Hinged Coloured Dust Cover-red
283	szt.	Patch Cord CU PA C6A S GY 3m
392	szt.	Easy Latch-green
174	szt.	Easy Latch-red
Gniazda Floorboxy Ciołka		
83	szt.	Mounting Plate 45x45 mm,2 port, flat-white
134	szt.	Module RJ45/s C6A ISO
102	szt.	Hinged Coloured Dust Cover-green
32	szt.	Hinged Coloured Dust Cover-red
134	szt.	Patch Cord CU PA C6A S GY 3m
204	szt.	Easy Latch-green
64	szt.	Easy Latch-red
Gniazda WIFi Ciołka (poziom 0)		
2	szt.	WM Global Outlet, 80x80,2x1 Port
2	szt.	Module RJ45/s C6A ISO
2	szt.	Plug Guard-white
2	szt.	FO Colour Clip SCRJ black
2	szt.	Patch Guard
2	szt.	FO Colour Clip SCRJ black
2	szt.	Patch Cord CU PA C6A S GY 1m
Szafy serwerownia		
3	szt.	Szafa serwerowa 19" 42U 800x1000 RAL 7035 standardowa
3	szt.	KPL.NAROŻNIKÓW COKOŁU 100
6	szt.	ŁĄCZNIK NAROŻNIKÓW PEŁNY /L- 600/ dł. ściany cokołu 800
6	szt.	ŁĄCZNIK NAROŻNIKÓW PEŁNY (L-800) dł. ściany cokołu 1000

3	szt.	Panel wentylacyjny z termostatem, RAL 7035
3	szt.	Zaślepka z włókniną i przepustem szczotkowym RAL 7035
12	szt.	Uchwyt kablowy 88x88 mm (komplet 5 szt.)
8	szt.	Łącznik do szaf
8	szt.	Listwa zasilająca z 5 gniazdami 2P+Z z filtrem sieciowym 30MHz
6	szt.	Półka regulowana 1U, gł. 500-900, RAL 7035
1	szt.	Przełacznica 1U-UniRack2-IR-12-lcdzpcBm-om3-dinvde
2	szt.	Splice holder 12 x heat shrink protect.
24	szt.	FO Splice protection Fujikura
1	szt.	FO Cable Guide 75mm for 19"1U Rack
12	szt.	Patch cord FO OM3 LCD/LCD 5m
24	szt.	Plug Guard for lcd connector
5	szt.	Patch panel HD-19" 1U-24xRJ45-C6A ISO/s-
13	szt.	Patch panel HD-19" 1U-24xRJ45-C6A ISO/s-
41	szt.	CM 1U 19" Metal Panel, Modular 70mm
298	szt.	HDS Level 1-HDC-green
119	szt.	HDS Level 1-HDC-red
417	szt.	Patch Cord CU PA C6A S GY 5m
596	szt.	Easy Latch-green
238	szt.	Easy Latch-red
2	szt.	HDS Level 3-Plug Guard-white
2	szt.	Patch Guard
2	szt.	FO Colour Clip SCRJ black
Kable		
23	km	Real10 S/FTP 4P 650 MHz LSZH
0,05	km	LT-cable-indoor-12-om3

Elementy aktywne telefonii IP

Ilość	Jednostka	Nazwa
1	Kpl	Serwer teleinformatyczny – wersja programowa (softswitch)
1	Kpl	Łącza miejskie SIP-Trunk 30-kanałów
300	Kpl	Łącza wewnętrzne cyfrowe IP
10	Kpl	Klient Unified Communication – samodzielna aplikacja na komputer PC lub MAC
5	Kpl	Klient UC jako dodatek do MS Outlook
10	Kpl	Dostęp do konferencji zaawansowanej dla klienta UC
128	Kpl	Wewnętrzna brama VoIP - ilość kanałów
1	Kpl	Zintegrowany system zapowiedzi słownych
42	Kpl	Dostęp do Wizualnej Poczty Głosowej dla abonenta
10	Kpl	Dostęp do osobistej skrzynki faksowej dla Klienta UC
10	Kpl	Użytkownik mobilny
10	Kpl	Dostęp do usługi „ Wspólne Biurko”
10	Kpl	Narzędzie do integracji z aplikacjami biznesowymi Zamawiającego
1	Kpl	Narzędzie do integracji z bazami danych Zamawiającego
1	Kpl	Multimedialne Contact Center (MCC):
1	Kpl	Obsługa kanału faksowego MCC
1	Kpl	Obsługa kanału e-mail MCC
10	Kpl	Aplikacja Agenta Contact Center
1	Kpl	Aplikacja Raporty
2	Kpl	Oprogramowanie stanowiska Awizo / Asystent
1	kpl	Aplikacja współpracująca z oprogramowaniem zarządzającym zgodnie z wymaganiami KRI
Aparaty telefoniczne cyfrowe:		

240	szt	W tym systemowe proste IP
10	Szt	W tym systemowe proste IP G
10	Szt	W tym systemowe sekretarskie IP G
10	Szt	W tym systemowe zaawansowane Contact Center IP G
10	Szt	W tym systemowe zaawansowany IP VIP
10	Szt	Przystawka rozszerzająca do min. 18 przycisków programowalnych
1	Kpl	Oprogramowanie rejestracji rozmów rejestrujące SIP Trunk 30-kanałowy
1	kpl	Oprogramowanie taryfikacji rozmów dla min. 300 abonentów,
2	Szt	Bramka VoIP 4 porty FXS z obsługą protokołu T.38
4	szt	Stanowisko komputerowe uniwersalne z Windows 10 Professional, monitor min. 22” full HD, klawiatura, mysz bezprzewodowa (2 stanowiska awizo, 1 stanowisko taryfikacji, 1 - administracji)

Elementy aktywne LAN

Ilość	Jednostka	Nazwa
GPD1		
2	szt	Przełącznik rdzeniowy
3	Szt	Moduł GBIC SR SFP+
2	Szt	Kabel krótki do łączenia w stos
1	Szt	Kabel zasilający min. 1,5 m C13
GPD2		
2	Szt	Przełącznik rdzeniowy
3	Szt	Moduł GBIC SR SFP+
2	Szt	Kabel krótki do łączenia w stos
1	Szt	Kabel zasilający min. 1,5 m C13
PD1-1		
2	Szt	Przełącznik 48 portowy uplink 10Gb
1	Szt	Przełącznik 48 portowy POE
1	Szt	Przełącznik 24 portowy
4	Szt	Kabel krótki do łączenia w stos
2	Szt	Kabel łączący stos z przełącznikiem rdzeniowym
4	Szt	Kabel zasilający min. 1,5 m C13
PD1-2		
2		Przełącznik 48 portowy uplink 10Gb
2		Przełącznik 48 portowy
2		Przełącznik 48 portowy POE
6		Kabel krótki do łączenia w stos
2		Kabel łączący stos z przełącznikiem rdzeniowym
6		Kabel zasilający min. 1,5 m C13
PD2-1		
2	Szt	Przełącznik 48 portowy uplink 10Gb
1	Szt	Przełącznik 48 portowy
1	Szt	Przełącznik 48 portowy POE
1	Szt	Przełącznik 24 portowy POE
5	Szt	Kabel krótki do łączenia w stos
2	Szt	Kabel łączący stos z przełącznikiem rdzeniowym
5	Szt	Kabel zasilający min. 1,5 m C13
PD2-2		
2	szt	Przełącznik 48 portowy uplink 10Gb
2	Szt	Przełącznik 48 portowy

2	Szt	Przełącznik 48 portowy POE
6	Szt	Kabel krótki do łączenia w stos
6	Szt	Kabel zasilający min. 1,5 m C13
2	Szt	Moduł GBIC SR SFP+
WLAN		
1	Zst	Kontroler sieci WLAN
2	szt	Punkt dostępowy sieci WLAN
Zarządzanie		
2	Kpl	System zarządzania siecią (NMS)
2	kpl	System kontroli dostępu - Network Access Controll (NAC)

6. System sygnalizacji włamania i napadu SSWiN

W budynku zakłada się wykonanie systemu sygnalizacji włamania i napadu zadaniem którego będzie ochrona przed włamaniem i napadem oraz automatyczne powiadamianie służb interwencyjnych w przypadku wystąpienia zagrożenia.

System sygnalizacji włamania i napadu SSWiN zostaną objęte następujące strefy:

- drzwi wejściowe do budynku,
- wszystkie pomieszczenia z oknami na parterze,
- wybrane pomieszczenia techniczne,
- wybrane pomieszczenia magazynowe,
- stanowiska obsługi (przyciski napadowe)

Ochrona pomieszczeń realizowana będzie przez zainstalowanie w tych pomieszczeniach czujek podczerwieni (PIR) lub czujek dualnych (PIR+MW) oraz czujek magnetycznych (kontaktronów). W wybranych miejscach zostaną zainstalowane klawiatury do sterowania (uzbrajania i rozbrajania systemu) poszczególnymi strefami dozorowymi.

Centralka systemu SSWiN zainstalowana jest w pomieszczeniu central dozorowych na poziomie -1 budynku przy ul. Ciołka.

7. System kontroli dostępu KD i rejestracji czasu pracy RCP

7.1 Ogólna charakterystyka systemu

W obiekcie zastosowano system kontroli dostępu połączony z systemem rejestracji czasu pracy, zadaniem którego będzie kontrolowanie ruchu osobowego oraz zabezpieczenie dostępu do wybranych stref/pomieszczenie osobom nieuprawnionym do wejścia.

System KD obejmuje swoim zasięgiem:

- wejścia do pokoi biurowych,
- wejścia do wybranych pomieszczeń technicznych,
- wejścia do serwerowni,
- wejścia wybranych pomieszczeń magazynowych,
- oddzielenie strefy po której poruszają się petenci od pozostałej strefy tylko dla urzędników

System RCP będzie gromadził i prezentował informację o czasie pracy, godzinach obecności, spóźnieniach i nadgodzinach. Rejestracja dokonuje się przez przyłożenie karty do rejestratora.

W chwili wystąpienia alarmu pożarowego w jakiejkolwiek strefie system będzie automatycznie zwalniał drzwi w danej strefie oraz na drogach ewakuacyjnych. Jeżeli system zawiedzie, tzn. nie otworzy drzwi na drogach ewakuacyjnych, to będzie istniała możliwość ręcznego zwolnienia drzwi przy pomocy awaryjnego przycisku wyjścia bądź klamki.

Do obsługi systemu przewiduje się zainstalowanie stacji komputerowej PC. System będzie umożliwiał wizualizacje systemu KD oraz RCP. Dodatkowo system będzie zapewniał dowolną obsługę systemów z poziomu PC tzn, drukowanie raportów, przyznawanie/zmiana dostępów, rejestracje zdarzeń, itd.

7.2 Wymagania systemu kontroli dostępu

- Dla celów kontroli dostępu wykorzystywany będzie element bezstykowy karty.
- Komunikacja w ramach systemu kontroli dostępu odbywać się będzie poprzez przez sieć LAN, WAN.
- Magistrale komunikacyjne zgodne z interfejsem zamontowanych urządzeń Kontroli Dostępu i Rejestracji czasu pracy tworzą lokalne węzły komunikacji. Elementem koncentrującym może być urządzenie sprzętowe lub aplikacja instalowana na określonym komputerze klasy PC, do którego podłączone są lokalne interfejsy urządzeń.
- Komunikacja z lokalnymi węzłami komunikacji a aplikacją nadzorującą odbywa się poprzez sieć pakietową z wykorzystaniem protokołów TCP/IP
- Komunikacja z urządzeniami realizowana jest w trybie on-line
- Elementy wykonawcze (elektrozaczepy, zwory magnetyczne, kontaktrony, samodomykacze i klamko-gałki), które zostaną zainstalowane na istniejących drzwiach Zamawiającego, powinny być dopasowane do estetyki zakładu.
- Wskazane przez Zamawiającego, czytniki powinny być wyposażone w klawiaturę.
- Wykorzystywane oprogramowanie w wersji sieciowej powinno bazować na istniejącej u Zamawiającego platformie bazodanowej MS SQL 2008.
- System kontroli dostępu musi pracować w sieci rozproszonej. Ewentualna utrata komunikacji ze sterownikiem w chronionym pomieszczeniu nie może paraliżować jego pracy.
- Zanik zasilania w sieci 230V nie może powodować utraty funkcjonalności systemu przez minimum 8 godzin.
- System powinien pozwalać na łatwą modułową rozbudowę o inne punkty.
- Aplikacja zarządzająca systemem kontroli dostępu musi posiadać następującą funkcjonalność: praca w architekturze klient/serwer, możliwość pracy jednostanowiskowej lub sieciowej, możliwość monitorowania wybranych czytników dla wybranych typów zdarzeń w czasie rzeczywistym, możliwość rejestracji pracy całego systemu, wywoływania pewnych akcji po wystąpieniu określonych zdarzeń, np. wyświetlenie komunikatu na ekranie programu, uruchomienia sygnału dźwiękowego w przypadku próby sforsowania drzwi, wysterowania dodatkowego modułu przekaźnikowego na komputerze klienckim, filtrowanie odczytów (rejestracji zdarzeń), przeglądanie ścieżek przejścia pracowników, stany osobowe stref, graficzną ilustrację rozkładu czytników w budynku, współpracę systemu z centralką alarmową i p.poż., sygnalizacja forsowania drzwi – sprzętowa i w oprogramowaniu, w tym możliwość współpracy z zewnętrznym systemem dozorowym,
- Odczytywanie rejestracji w sposób ciągły zapewniający stały dostęp do aktualnych zdarzeń w kontrolowanym systemie, a także o określonych, dowolnie zdefiniowanych godzinach (np. dwa razy na dobę). System po rozpoczęciu komunikacji okresowej ma przeprowadzać pobieranie danych zgromadzonych na urządzeniach do momentu opróżnienia lokalnych buforów danych na każdym z urządzeń
- Umożliwienie kontroli pracy systemu, nadawania uprawnień poszczególnym użytkownikom, modyfikację reguł dostępu do określonych pomieszczeń, sporządzanie raportów,
- Możliwość stałego zablokowania lub odblokowania drzwi przez operatora w dowolnym przedziale czasu,
- System kontroli dostępu oferowany jest razem z integracją z systemem Rejestracji Czasu Pracy (RCP) w oparciu o wspólną bazę pracowników, przy wykorzystaniu tych samych kart elektronicznych, oraz zarządzanie wspólnym zestawem czytników mogących współdzielić funkcje rejestracji czasu pracy i kontroli dostępu,
- Czasową lub stałą blokadę wybranych kart. Informacja o zablokowaniu użytkownika powinna być realizowana automatycznie poprzez synchronizację z systemem AD (baza danych użytkowników poprzez protokół LDAP).
- Aplikacja ma mieć możliwość określenia dodatkowych parametrów opisujących grupy pracowników.

7.3 Wymagania systemu rejestracji czasu pracy

- Oprogramowanie rejestracji czasu pracy musi być oprogramowaniem zintegrowanym z systemem kontroli dostępu na poziomie:
    - wspólnej bazy danych
    - wspólnej bazy użytkowników systemu – identyfikowanych przez karty zbliżeniowe
    - wspólnej bazy urządzeń, z których wybrane urządzenia mogą pełnić rolę zarówno urządzeń Kontroli Dostępu jak i Rejestracji Czasu Pracy (RCP)
    - wspólnej listy operatorów aplikacji z możliwością wyszczególnienia poziomu dostępu
- Aplikacja ma umożliwiać rozliczenie czasu pracy zgodnie z aktualnie obowiązującym Kodeksem Pracy
- Aplikacja ma umożliwiać definiowanie nielimitowanej drzewiastej struktury firmy z możliwością przydzielenia pracowników do każdego elementu drzewa

- Operatorzy mogą zdefiniować dla określonej grupy pracowników harmonogram pracy, względem którego zostanie rozliczony czas pracy
- W celu przyśpieszenia obliczeń, aplikacja ma posiadać osobne oprogramowanie działające w trybie usługi systemowej odpowiedzialne za główny algorytm rozliczający.
- Aplikacja udostępnia wyniki rozliczenia czasu pracy w formie raportów dostępnych z aplikacji jak i poprzez przeglądarkę internetową
- Tworzenie harmonogramów pracy powinno być zautomatyzowane. Aplikacja powinna umożliwiać definiowanie szablonów, według których automatycznie będą tworzone harmonogramy pracy.
- Operatorzy powinni mieć możliwość bezpośredniej edycji harmonogramów pracy.
- Aplikacja musi samodzielnie obliczać normatywny czas pracy oraz umożliwiać prawidłowe rozliczanie pracowników pracujących w niepełnym wymiarze godzin.
- Aplikacja ma mieć możliwość zdefiniowania zezwoleń dla pracowników rozszerzających standardowy przyznany pracownikowi czas pracy. Minimalnymi typami zezwoleń są: Wyjście służbowe, wcześniejsze wyjście służbowe, nadgodziny, modyfikacja godziny przyjścia do pracy, praca w dzień wolny.
- Aplikacja musi posiadać moduł automatycznego wykrywania błędów w rejestracjach (np. brak rejestracji przy wejściu lub przy wyjściu,
- Aplikacja ma umożliwiać rozliczanie pracowników pracujących według różnych systemów pracy. Dla każdego systemu pracy aplikacja ma umożliwiać zdefiniowanie nielimitowanej ilości harmonogramów pracy. Harmonogram ma mieć możliwość ograniczenia czasowego wraz z określeniem normatywnych godzin pracy. Harmonogram ma mieć możliwość określenia do 4 zmian.
- Aplikacja RCP ma mieć możliwość zmiany, dodania i edycji rejestracji, na podstawie których obliczany jest czas pracy pracowników. Modyfikacje rejestracji nie mogą wpływać na dane rzeczywistych rejestracji powstałych w procesie używania kart zbliżeniowych.
- Aplikacja musi przeprowadzać analizę rejestracji wykorzystywanych do rozliczenia czasu pracy. Analiza ma umożliwiać znalezienie błędnych rejestracji pod względem rozliczenia czasu pracy wraz z zaproponowaniem alternatywnych rozwiązań umożliwiających dodanie brakującej rejestracji, edycji trybu lub kierunku rejestracji. Aplikacja powinna umożliwić korektę i weryfikację rejestracji na urządzeniach niezależnie od finalnego rozliczenia czasu pracy zgodnie z przydzielonym harmonogramem czasu pracy.
- Aplikacja ma mieć możliwość określenia okresu rozliczeniowego z dokładnością do tygodnia.
- Aplikacja ma wspierać następujące systemy czasu pracy: podstawowy, równoważny, ciągły, weekendowy.

7.4 Charakterystyka techniczna urządzeń

Sterowniki KD

- Obsługa jednego, dwóch, czterech lub maksymalnie 20czytników (magnetycznych, zbliżeniowych lub biometrycznych) z interfejsem ABA Track II lub Wiegand po zastosowaniu modułów I/O (rozszerzających).
- Komunikacja pomiędzy sterownikiem, a modułami I/O za pomocą magistrali CAN,
- Pamięć wewnętrzna minimum 128kB zegar RTC w systemie 24H,
- Czas podtrzymania RAM i zegara minimum 120h po zaniku napięcia zasilania,
- Sygnalizacja za pomocą diod LED lub wyświetlacza LCD, możliwa akustyczna
- Komunikacja szeregowa asynchroniczna RS232, RS485 lub Ethernet (w zależności od wersji),
- Zasilanie 12V-16V, maksymalny pobór prądu 300mA bez czytnika w zależności od wersji,
- Wejście PPOŻ, wejście informacyjne o zasilaniu awaryjny, konfigurowane wyjścia NO/NC,
- Obudowa zabezpieczona kluczem,
- Możliwość pracy w temperaturze -10 – 50 st, wilgotność poniżej 80%.

Rejestrator RCP/KD

- Obsługa jednego lub dwóch czytników (magnetycznych, zbliżeniowych lub biometrycznych) z interfejsem ABA Track II lub Wiegand,
- Klawiatura 16 klawiszowa,
- Wyświetlacz LCD 32 znakowy,
- Pamięć wewnętrzna minimum 512kB, zegar RTC w systemie 24H,
- Czas podtrzymania RAM i zegara minimum 120h po zaniku napięcia zasilania,
- Sygnalizacja za pomocą diod LED lub akustyczna,

- Komunikacja szeregowa asynchroniczna RS232, RS485 lub Ethernet (w zależności od wersji),
- Zasilanie 12V, maksymalny pobór prądu 300mA bez czytnika,
- Wejście PPOŻ, wejście informacyjne o zasilaniu awaryjnym, konfigurowane wyjścia NO/NC,
- Możliwość pracy w temperaturze -10 – 50 st, wilgotność poniżej 80%,
- Mocowanie antysabotażowe.

Czytniki KD Zbliżeniowe

- Dostępne wersje natynkowe i podtynkowe oraz z klawiaturą,
- Obsługa kart zbliżeniowych MIFARE,
- Interfejs komunikacyjny ABA TRACK II lub Wiegand,
- Sygnalizacja za pomocą diod LED (dwukolorowa) i akustyczna,
- Obudowa hermetyczna odporna na niekorzystne warunki atmosferyczne,
- Zasilanie 12V po przewodzie komunikacyjnym ze sterownika,
- Możliwość pracy w temperaturze -25 – 55 st, wilgotność poniżej 80%.

Zasilacz buforowy

- Napięcie wejściowe 160-260V AC,
- Napięcie wyjściowe 12V regulowane,
- Zabezpieczenie przed całkowitym rozładowaniem akumulatora,
- Obsługa akumulatora 12V 7Ah,
- Zabezpieczenie obwodu wejściowego i wyjściowego,
- Sygnalizacja stanu akustyczna i diodami LED,
- Styk informacyjny pracy z akumulatora Interfejs komunikacyjny ABA TRACK II lub Wiegand,
- Sygnalizacja za pomocą diod LED (dwukolorowa) i akustyczna.

Elektrozaczep

- Napięcie zasilania 12DC, pobór prądu max 300mA,
- Praca rewersyjna,
- Możliwość montażu symetrycznego,
- Regulowana zapadka,

Zwora magnetyczna

- Napięcie zasilania 12/24DC, pobór prądu max 600mA przy 12V,
- Czujnik halla,
- Minimalna siła trzymania 3000N,
- Możliwość zamocowania przy pomocy elementów montażowych typu Z, L itp.
- Optyczna sygnalizacja stanu.

Kontaktron

- Magnetyczny,
- Montaż nawierzchniowy lub wpuszczany w zależności od drzwi.

Przycisk wyjścia ewakuacyjny

- Montaż natynkowy,
- Wyzwolenie alarmu poprzez naciśnięcie szybki,
- Odblokowanie za pomocą dedykowanego klucza,
- Styki sygnalizacji użycia.

8. Instalacja telewizji dozorowej CCTV

W obiekcie zakłada się wykonanie instalacji telewizji dozorowej zadaniem którego będzie nadzór wizyjny nad wybranymi i newralgicznymi strefami w budynku i na terenie zewnętrznym.

Przewiduje się że system CCTV obejmowałby swoim zasięgiem następujące przestrzenie:

- hole główne i strefy obsługi Interesantów,
- główne ciągi komunikacji w budynku,
- klatki schodowe,
- wybrane newralgiczne pomieszczenia i obszary w budynku,
- elewacje budynku i teren zewnętrzny przyległy do obiektu,

Szafa Rack CCTV będzie znajdować się w pomieszczeniu central dozoru. Będzie składać się z kompletu elementów zapewniających rejestracje i archiwizację danych.

W systemie zakłada się zastosowanie kamer z funkcją dzień-noc (oświetlaczem podczerwieni) oraz detekcją ruchu w celu zmniejszenia zapotrzebowania na przestrzeń dyskową. Projektuje się 30-dniową archiwizacje danych.

Wszystkie kamery zewnętrzne muszą być wyposażone w obudowy hermetyczne wyposażone w grzałkę i termostat oraz ewentualnie zasilacz.

9. System kolejkowy

Wymagania główne

System kolejkowy będzie obejmował łącznie 10 stanowisk obsługi i musi umożliwiać tworzenie nieograniczonej ilości kolejek. Systemem musi sterować jeden serwer systemu.
Elementy systemu usytuowane będą w miejscach oznaczonych na planach systemów bezpieczeństwa (SB)

Elementy systemu

Zleceniobiorca dostarczy:

a. Automat biletowy min 19 cali – szt. 1 służący do wydawania biletów
b. Terminale stanowiskowe sprzętowe – 10 szt.
c. Wyświetlacze stanowiskowe LED lub LCD - 10 szt.
d. Wyświetlacz wielkoformatowy (monitor wielkoformatowy 50") – 2 komplety
e. Wyświetlacz wielkoformatowy reklamowy (monitor wielkoformatowy 50") – 1 komplet (z możliwością przekształcenia, w monitor systemu numerkowego).
f. Oprogramowanie spełniające warunki określone w szczegółowym opisie funkcjonalnym.
g. Instalacja oraz zestaw do połączeń wzajemnych poszczególnych części systemu (okablowanie, switche i inne) - 1 komplet.
h. Serwer systemu

Dodatkowe funcjonalności systemu:

i. Umawianie wizyt przez Internet
j. Umawianie wizyt w placówce
k. Podgląd stanu kolejki on-line

Szczegółowy opis funkcjonalny

a. <u>Automat biletowy</u>

System zawiera automat biletowy, stojący, o wys. min. 145 cm i max. 155 cm. Biletomat powinien zapewnić łatwą wymianę papieru. Powinien być zaopatrzony w panel dotykowy, z nakładką dotykową typu pojemnościowego umożliwiający programowanie dowolnej ilości przycisków oraz umieszczanie na bilecie dowolnych informacji z systemu np. numer klienta, znak graficzny, data, przewidywany czas oczekiwania, przewidywana godzina wezwania, liczba oczekujących. Biletomat ma umożliwiać łatwy dostęp dla osób niepełnosprawnych, np. na wózkach inwalidzkich.

Wybieranie poszczególnych kolejek powinno być możliwe w trybie wieloekranowym (menu hierarchiczne) np. przycisk główny „rejestracja” → „rejestracja dla osób A – H” i → „rejestracja dla osób I-Z”. Pobranie biletu z automatu biletowego będzie się odbywało przez naciśnięcie monitora dotykowego w miejscu, które wyświetla przycisk kolejki.

Ekran dotykowy powinien umożliwiać pobranie biletu po rezerwacji wizyty przez Internet, poprzez wprowadzenie kodu niezbędnego do wydrukowania zarezerwowanego biletu.

Zamawiający powinien mieć możliwość redagowania informacji umieszczonych na drukowanych przez automat biletach: np. numer klienta, znak graficzny, data, przewidywany czas oczekiwania, liczba oczekujących.

Oprogramowanie ma mieć możliwość automatycznego lub ręcznego aktualizowania przez Internet–a dostawca dostarczy bezpłatne aktualizacje systemu, co najmniej przez czas trwania gwarancji.

b. Terminale stanowiskowe – sprzętowe

System musi zapewnić możliwość przywoływania interesantów do stanowisk za pomocą terminali stanowiskowych sprzętowych dedykowanych do systemów kolejkowych (zamawiający nie dopuszcza użycia tabletów itp. urządzeń)
Panel przywoławczy ma służyć do:

- logowania pracowników poprzez wprowadzenie osobistego kodu umożliwiającego przypisanie danych statystycznych do pracownika
- przywołania klienta kolejnego i wybranego w tym pobierania klientów z kolejek obsługiwanych na innych stanowiskach pracy.
- przekierowania klientów między stanowiskami i kolejkami
- wstrzymania obsługi dowolnego klienta i zawieszenia jego obsługi do wezwania
- ponownego przywołania numeru biletu, który się nie stawił
- podawania informacji o stanie kolejki (liczba oczekujących)
- wyłączenia stanowiska z pracy

c. Wyświetlacze stanowiskowe LED lub LCD

Wyświetlacz obsługujący stanowisko pracy, pozwalający obserwować kolejne wzywane numery do stanowiska pracy. Wysokość pojedynczego znaku na wyświetlaczu powinna zapewnić dobrą czytelność dla klientów. Wyświetlacz powinien wyświetlać:

- numer biletu w układzie czteroznakowym z prefiksem literowym A123

d. Wyświetlacze wielkoformatowe (42;" 50")

Wyświetlacze wielkoformatowe pracujące w trybie 16/24h Zamawiający nie dopuszcza użycia telewizorów.

Na ekranie będą wyświetlane informacje dotyczące aktualnie wzywanych numerów (dowolna mieszcząca się na ekranie ilość) oraz opcjonalnie także informacje skierowane do Klientów w układzie graficznym wybranym przez placówkę, w zależności od ustawień dokonanych przez użytkownika.

e. Umawiane wizyt przez Internet samodzielnie przez klientów

System powinien być wyposażony w funkcjonalność umawiania wizyt przez Internet na dni następne (w ustalonym zakresie czasowym). System powinien umożliwiać:

- rezerwowanie biletów bez konieczności posiadania jakiegokolwiek konta w systemie rezerwacyjnym
- zabezpieczenie przed działaniem automatycznych systemów internetowych (botów), które automatycznie będą pobierały bilety
- zbieranie danych rezerwacyjnych do lokalnej bazy danych na stronie urzędu (np. MySQL) i dalsze synchronizowanie w taki sposób, aby kontrolować w urzędzie proces umawiania wizyt
- otrzymanie na zakończenie procesu rezerwacji (gdzie klient wybiera dzień, godzinę i kolejkę) automatycznego maila lub SMS-a, z informacją o numerze rezerwacji i sposobie dalszego postępowania.
- możliwość anulowania wizyty przez klienta

f. Umawianie wizyt w urzędzie

System powinien być wyposażony w funkcjonalność umawiania wizyt przez pracownika w urzędzie na dni następne. System powinien umożliwiać:

- rezerwowanie biletów
- otrzymanie na zakończenie procesu rezerwacji informacji w postaci komunikatu lub wydruku dotyczącego numeru rezerwacji i sposobie dalszego postępowania.
- możliwość anulowania wizyty.

Ta funkcjonalność powinna być dostępna dla nieograniczonej ilości użytkowników bez ponoszenia dodatkowych kosztów.

g. Podgląd stanu kolejki on line.

Możliwość podglądu on-line stanu kolejki w urzędzie (ilość osób obsłużonych, ilość oczekujących, średni czas oczekiwania, bieżący numer obsługiwany)

h. Oprogramowanie systemu kolejkowego

Oprogramowanie musi spełniać następujące wymagania:

- oprogramowanie klienckie systemu, uruchamiane na komputerze użytkownika, musi pracować w środowisku Windows, aktualnie wspieranym przez jego producenta
- system powinien działać na serwerze bez konieczności jego ręcznego uruchamiania.
- system powinien być zabezpieczony hasłami w celu ochrony danych, wg różnych poziomów uprawnień (administrator, kierownik, pracownik).
- system powinien umożliwiać tworzenie nieograniczonej ilości kolejek i grupowania ich w grupy
- system powinien umożliwiać tworzenie różnych scenariuszy obsługi, w zakresie których pewne kolejki są obsługiwane szybciej (z priorytetem na wybranych stanowiskach lub grupach stanowisk)
- każde stanowisko może obsługiwać więcej niż jedna kolejkę.
- system powinien umożliwiać dowolny transfer klientów pomiędzy różnymi stanowiskami bez konieczności ponownego pobierania biletu.
- w przypadku zaniku napięcia, po ponownym uruchomieniu system powinien zapewniać automatyczne uruchomienie, z utrzymaniem ciągłości kolejki.
- system powinien zapewniać wydawanie biletów w ramach ustalanych harmonogramów godzinowych (w godzinach pracy wskazanych przez Zamawiającego) lub w zakresie puli dziennej lub dynamicznie w taki sposób, aby wydawać bilety tylko tym klientom, których można obsłużyć w godzinach pracy urzędu. Administrator dodatkowo powinien mieć możliwość blokowania wydawania biletów do całości systemu lub do każdej kolejki z osobna.
- powinna istnieć możliwość blokowania wydawania biletów w sytuacji, kiedy spodziewany czas obsługi wykracza poza godziny pracy systemu.
- system powinien umożliwiać umawianie wizyt na bieżący i kolejne dni zarówno poprzez Internet jak i u pracownika.
- system powinien generować zapowiedzi słowne informujące o zaproszeniu klienta do stanowiska. Zapowiedź powinna zawierać numer biletu, numer stanowiska, numer pokoju, numer piętra i inne.
- System ma posiadać moduł raportów i analiz, umożliwiający zbieranie i przetwarzanie wszelkich danych statystycznych o pracy, takich jak:
- ilość wykonywanych operacji w podziale na rodzaje, stanowiska obsługi oraz personel w określonym przedziale czasu,
- wydajność pracy poszczególnych pracowników indywidualnych (liczba obsłużonych klientów, efektywnie przepracowany czas, czas przerw itp.)
- czas oczekiwania na obsługę,
- czas obsługi klientów,
- czas realizacji poszczególnych typów operacji.
- Wymagane jest również, aby:
- moduł statystyczny był w języku polskim.
- oprogramowanie ma mieć możliwość automatycznego lub ręcznego aktualizowania przez Internet a dostawca dostarczy bezpłatne aktualizacje systemu co najmniej przez czas trwania gwarancji.
- powinna być możliwość zbierania i wyświetlania raportów statystycznych zarówno w trybie online jak i historycznym

i. Instalacja oraz zestaw do połączeń wzajemnych poszczególnych części systemu (okablowanie, switche i inne) - 1 komplet.

j. Wymagania dotyczące statystyk.

System ma mieć możliwość zbierania i przetwarzania wszelkich danych statystycznych o pracy Urzędu, w szczególności:

- ilość i czas wydawania numerów w określonym przedziale czasu
- ilość wykonywanych operacji w podziale na rodzaje, stanowiska obsługi oraz personel w określonym przedziale czasu,

- wydajność pracy poszczególnych pracowników (liczba obsłużonych klientów),
- czasy oczekiwania na obsługę, w tym średnie, minimalne, maksymalne
- czasy obsługi klientów, w tym średnie, minimalne, maksymalne
- czasy realizacji poszczególnych typów operacji,
- drukowanie i eksportowanie do xls, raportów statystycznych
- tworzenie własnych dowolnych własnych raportów nie ujętych w powyższym zestawieniu

Ta funkcjonalność powinna być dostępna dla nieograniczonej ilości użytkowników bez ponoszenia dodatkowych kosztów.

k. Możliwość rozbudowy systemu.

System powinien zapewnić możliwość rozbudowy każdego z jego elementów składowych,

10. System BMS

W budynku przewiduje się zastosowanie centralnego systemu monitorowania i sterowania instalacji i urządzeń technicznych BMS.
Przewiduje się możliwość całkowicie autonomicznej pracy systemów lokalnych, a także ich współpraca z systemem BMS, nadrzędnie monitorującym i kontrolującym systemy lokalne.
Na komputerze centralnym zostanie zainstalowane oprogramowanie, umożliwiające odbieranie i wysyłanie sygnałów za pośrednictwem okablowania magistralnego, do modułów lokalnych, współpracujących z urządzeniami systemów lokalnych, m.in. w instalacji elektrycznej, wentylacji i klimatyzacji, systemu sygnalizacji pożaru, kontroli dostępu, itp.
Jednostka centralna będzie współpracowała z jednostkami operatorskimi, wyposażonymi w interfejs wizualizacji zdarzeń (tzw. maski graficzne dla każdego z systemów). Z pomocą jednostek operatorskich możliwe będzie odczytywanie i zadawanie wartości właściwych wielkości parametrów fizycznych w obiekcie.
System będzie rejestrował i przechowywał wyniki pomiarów oraz informacje o zdarzeniach w bazie danych.
Zasilanie systemu BMS będzie się odbywało z części rozdzielnicy gwarantującej zasilanie rezerwowe oraz poprzez indywidualny zasilacz UPS.

11. Prowadzenie instalacji teletechnicznych

- Przepusty instalacyjne w elementach oddzielenia przeciwpożarowego powinny mieć klasę odporności ogniowej (E I 120) wymaganą dla tych elementów.
- Dopuszcza się nie instalowanie przepustów, o których mowa w pkt. 1, dla pojedynczych rur instalacji wodnych, kanalizacyjnych i ogrzewczych, wprowadzanych przez ściany i stropy do pomieszczeń higieniczno sanitarnych.
- Przepusty instalacyjne o średnicy powyżej 4 cm w ścianach i stropach, nie wymienionych w pkt. 1, dla których jest wymagana klasa odporności ogniowej co najmniej EI 60 lub REI 60, powinny mieć klasę odporności ogniowej (EI 60) tych elementów.
- Przepusty instalacyjne o średnicy większej niż 0,04 m w ścianach i stropach pomieszczenia zamkniętego, dla których wymagana klasa odporności ogniowej jest nie niższa niż EI 60 lub REI 60, a nie będących elementami oddzielenia przeciwpożarowego, powinny mieć klasę odporności ogniowej (EI 60) ścian i stropów tego pomieszczenia.
- Przejścia instalacji przez zewnętrzne ściany budynku, znajdujące się poniżej poziomu terenu, powinny być zabezpieczone przed możliwością przenikania gazu do wnętrza budynku.
- Projektuje się połączenie teletechniczne międzybudynkowe.
- Instalacje należy ułożyć w pasach zieleni i w strefie utwardzenia. Pod drogami i ciągami pieszymi stosować rury osłonowe.
- Instalacje elektryczne i teletechniczne zewnętrze oraz instalacje oświetleniowe pokazano na wspólnym rysunku PZT.
- Istniejące przebudowywane budynki posiadają przyłącze telekomunikacyjne operatora ORANGE POLSKA.

12. Plan BIOZ

Podstawą opracowania są następujące wytyczne:

Informacja dotycząca bezpieczeństwa i ochrony zdrowia (BIOZ)

Zgodnie z Rozporządzeniem Ministra Infrastruktury z dn.2002.06.23/Dz.U.NR 120poz. 1126/„W sprawie informacji dotyczącej bezpieczeństwa i ochrony zdrowia oraz planu bezpieczeństwa i ochrony zdrowia", podaje się informacje, które winny być zawarte w „planie bioz".

Informacja dotycząca bezpieczeństwa i ochrony zdrowia (BIOZ) – INFORMACJE OGÓLNE

Charakter robót budowlanych prowadzonych przy realizacji inwestycji stwarza ryzyko powstania zagrożenia bezpieczeństwa i zdrowia ludzi.

Przy prowadzeniu robót budowlanych należy:

- Wydzielić teren na którym prowadzone będą roboty przed dostępem osób postronnych.
- Oznakować miejsca prowadzenia prac.
- Urządzenia i instalacje energetyczne stwarzające zagrożenia dla zdrowia i życia ludzkiego należy zabezpieczyć przed dostępem osób nieupoważnionych.
- Miejsce przy urządzeniach energetycznych powinno być właściwie przygotowane, oznaczone i zabezpieczone w sposób określony w ogólnych przepisach bezpieczeństwa i higieny pracy.
- W każdym miejscu pracy, w którym wykonuje pracę zespół pracowników, powinien być wyznaczony kierujący tym zespołem.
- Wyłączenie urządzeń i instalacji elektroenergetycznych spod napięcia powinno być dokonane w taki sposób, aby uzyskać przerwę izolacyjną w obwodach zasilających urządzenia i instalacje.
- Prace w warunkach szczególnego zagrożenia dla zdrowia i życia ludzkiego, określone w ogólnych przepisach bezpieczeństwa i higieny pracy jako prace szczególnie niebezpieczne, powinny być wykonywane co najmniej przez dwie osoby, z wyjątkiem prac eksploatacyjnych z zakresu prób i pomiarów, konserwacji i napraw urządzeń i instalacji elektroenergetycznych o napięciu znamionowym do 1 kV, wykonywanych przez osobę wyznaczoną na stałe do tych prac w obecności pracownika asekurującego, przeszkolonego w udzielaniu pierwszej pomocy.
- Do robót używać sprzęt posiadający atesty. Stan techniczny narzędzi pracy i sprzętu ochronnego należy sprawdzać bezpośrednio przed jego użyciem. Narzędzia pracy i sprzęt ochronny, niesprawne lub które utraciły ważność próby okresowej, powinny być niezwłocznie wycofane z użycia.
- Prace pod napięciem należy wykonywać w oparciu o właściwą technologię pracy i przy zastosowaniu wymaganych narzędzi i środków ochronnych, określonych w instrukcji wykonywania tych prac.

- Przed przystąpieniem do wykonywania prac przy urządzeniach i instalacjach elektroenergetycznych wyłączonych spod napięcia należy:
  - o zastosować odpowiednie zabezpieczenie przed przypadkowym załączeniem napięcia,
  - o wywiesić tablicę ostrzegawczą w miejscu wyłączenia obwodu o treści: "Nie załączać",
  - o sprawdzić brak napięcia w wyłączonym obwodzie,
  - o uziemić wyłączone urządzenia,
  - o zabezpieczyć i oznaczyć miejsce pracy odpowiednimi znakami i tablicami ostrzegawczymi.

- Prace rozruchowe, próby techniczne urządzeń i instalacji energetycznych powinny być prowadzone zgodnie z wymaganiami Polskich Norm, odrębnych przepisów, instrukcji eksploatacji oraz uzgodnione z ich użytkownikiem.
- Prace w warunkach szczególnego zagrożenia dla zdrowia i życia ludzkiego należy wykonywać na podstawie polecenia pisemnego, przy zastosowaniu odpowiednich środków zabezpieczających zdrowie i życie ludzkie.
- Zapewnić wykonawstwo robót przez pracowników posiadających aktualne badania lekarskie i wysokościowe oraz spełniający odpowiednie wymagania kwalifikacyjne dla rodzajów wykonywanych prac i zajmowanych stanowisk (zgodnie z Rozporządzeniem Ministra Gospodarki, Pracy i Polityki Społecznej z dnia 28.04.2003r.
- Zapewnić nadzór nad budową przez osobę uprawnioną
- Zapewnić wszelkie wymagania z zakresu bezpieczeństwa i higieny pracy.

Informacja dotycząca bezpieczeństwa i ochrony zdrowia (BIOZ) dla instalacji teletechnicznych

1. Zakres robót i kolejność realizacji:
   - montaż tras koryt i drabin kablowych,
   - ułożenie instalacji teletechnicznych,
   - montaż tablic i szaf teletechnicznych
   - montaż osprzętu z podłączeniem,
   - sprawdzenie instalacji teletechnicznej,
   - pomiary instalacyjne,
   - próby i uruchomienie instalacji.

2. Wykaz istniejących obiektów budowlanych w pasie prowadzonych robót
   - w pasie prowadzonych robót występuje uzbrojenie budynku w instalacje: elektryczne, wodnokanalizacyjne, co.

3. Elementy zagospodarowania mogące stwarzać zagrożenie bezpieczeństwa i zdrowia ludzi:
   - niezabezpieczone przejścia,
   - drabiny, rusztowania,
   - pozostawione materiały i narzędzia,
   - instalacje elektryczne placu budowy,
   - spadające i występujące elementy w trakcie prowadzonych prac montażowych,
   - wykopy.

4. Przewidywane zagrożenia występujące podczas realizacji robót

Skala	Rodzaj zagrożenia	Miejsce	Czas występowania
Niska	potrącenie pojazdem mechanicznym	plac budowy	podczas wykonywania robót
Średnia	wpadnięcie do wykopu	wykopy pod sieci, uziemienie	podczas wykonywania robót
Średnia	przygniecenie	w miejscu załadunku, rozładunku i wykonania	podczas wykonania robót rozładunkowych i wykonywania instalacji
Średnia	upadek z wysokości	w budynku i na zewnątrz budynku	podczas wykonywania instalacji elektrycznych oraz inst. odgromowej
Średnia	natrafienie na wystające elementy	w budynku	od czasu rozpoczęcia prac do ich zakończenia
Średnia	porażenie prądem elektrycznym	w miejscu realizacji, prac, rozdzielnie elektryczne, wykonanie pomiarów elektrycznych	podczas wykonywania prac, pomiarów elektrycznych

5. Informacja o sposobie prowadzenia instruktażu pracowników:
   - przed przystąpieniem do robót zapoznać pracowników z zakresem, charakterem i sposobem prowadzenia robót oraz o występujących zagrożeniach wynikających z projektu budowlanego,
   - pouczyć pracowników o sposobie zachowania się w przypadku wystąpienia zagrożeń,
   - instruktaż stanowiskowy winien być odnotowany w zeszycie instruktaży,
   - pracownicy w zakresie pełnionych obowiązków i posiadanej specjalizacji muszą posiadać zaświadczenia kwalifikacyjne i uprawnienia zawodowe.

6. Środki techniczne i organizacyjne zapobiegające niebezpieczeństwom wynikającym z wykonania robót w strefach szczególnego zagrożenia:
   - wyposażyć pracowników w środki ochrony osobistej: rękawice, kaski i okulary ochronne,
   - teren prowadzenia prac pod napięciem wygrodzić taśma biało czerwoną, zawieszoną na wysokości 0,6-0,8m i tablicami ostrzegawczymi,
   - wyposażenie pracowników w środki łączności.

7. Wskazanie miejsca przechowywania dokumentacji:

- projekt budowlany, dziennik, lista obecności oraz zeszyt instruktaż winny znajdować się w biurze budowy,
- pisemne polecenie na prace w pobliżu czynnych urządzeń elektroenergetycznych, winny być w posiadaniu brygadzisty.

Projektował:
mgr inż. Krzysztof Gantzki
nr upr. WA-43/01

Sprawdził:
mgr inż. Michał Szymanowicz
nr upr. MAZ/0260/PBE/15

13. Zestawienie rysunków

L.p.	Sygnatura rysunku							Nazwa	Skala
1	PAS	130	PW	IN	SSP	R	01	Rzut instalacji SSP – poziom -1	1:100
2	PAS	130	PW	IN	SSP	R	02	Rzut instalacji SSP – poziom 0	1:100
3	PAS	130	PW	IN	SSP	R	03	Rzut instalacji SSP – poziom +1	1:100
4	PAS	130	PW	IN	SSP	R	04	Rzut instalacji SSP – poziom + 2	1:100
5	PAS	130	PW	IN	SSP	R	05	Rzut instalacji SSP – poziom +3	1:100
6	PAS	130	PW	IN	SSP	R	06	Rzut instalacji SSP – poziom +4	1:100
7	PAS	130	PW	IN	SSP	R	07	Rzut instalacji SSP – poziom dachu	1:100
8	PAS	130	PW	IN	LAN	R	01	Rzut instalacji sieci strukturalnej – poziom -1	1:100
9	PAS	130	PW	IN	LAN	R	02	Rzut instalacji sieci strukturalnej – poziom 0	1:100
10	PAS	130	PW	IN	LAN	R	03	Rzut instalacji sieci strukturalnej – poziom +1	1:100
11	PAS	130	PW	IN	LAN	R	04	Rzut instalacji sieci strukturalnej – poziom +2	1:100
12	PAS	130	PW	IN	LAN	R	05	Rzut instalacji sieci strukturalnej – poziom +3	1:100
13	PAS	130	PW	IN	LAN	R	06	Rzut instalacji sieci strukturalnej – poziom +4	1:100
14	PAS	130	PW	IN	SB	R	01	Rzut instalacji systemów bezpieczeństwa – poziom -1	1:100
15	PAS	130	PW	IN	SB	R	02	Rzut instalacji systemów bezpieczeństwa – poziom 0	1:100
16	PAS	130	PW	IN	SB	R	03	Rzut instalacji systemów bezpieczeństwa – poziom +1	1:100
17	PAS	130	PW	IN	SB	R	04	Rzut instalacji systemów bezpieczeństwa – poziom +2	1:100
18	PAS	130	PW	IN	SB	R	05	Rzut instalacji systemów bezpieczeństwa – poziom +3	1:100
19	PAS	130	PW	IN	SB	R	06	Rzut instalacji systemów bezpieczeństwa – poziom +4	1:100
20	PAS	130	PW	IN	SSP	SCH	1.0	Schemat instalacji systemu SSP w budynku przy ul. Astronomów	-
21	PAS	130	PW	IN	SSP	SCH	1.1	Schemat instalacji systemu SSP w budynku przy ul. Ciołka	-
22	PAS	130	PW	IN	ODD	SCH	2	Schemat instalacji oddymiania grawitacyjnego	-
23	PAS	130	PW	IN	KOL	SCH	3	Schemat instalacji kolejkowej	-
24	PAS	130	PW	IN	SSWIN	SCH	4	Schemat instalacji sygnalizacji włamania i napadu	-
25	PAS	130	PW	IN	KD	SCH	5	Schemat instalacji kontroli dostępu	-
26	PAS	130	PW	IN	LAN	SCH	6	Schemat instalacji sieci strukturalnej	-
27	PAS	130	PW	IN	CCTV	SCH	7	Schemat instalacji telewizji dozorowej	-
28	PAS	130	PW	IN	LAN	WID	1	Widok szaf teleinformatycznych	-

14. Oświadczenie projektantów

15. Uprawnienia projektantów