

## **OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia jest budowa nowego systemu telewizji dozorowo – użytkowej w Bazie Transportu Biura Gospodarczego Najwyższej Izby Kontroli przy ulicy Gagarina 3 w Warszawie.

Budowa systemu obejmuje dostawę oraz przeniesienie na Zamawiającego fabrycznie nowych, bez śladów użytkowania urządzeń i komponentów systemu CCTV IP oraz wykonanie prac montażowych, konfigurację przedmiotowego systemu i demontaż obecnie eksploatowanego systemu.

Zdemontowane elementy systemu CCTV należy przekazać Zamawiającemu.

Wykonawca zamontuje urządzenia i komponenty systemu CCTV IP w miejscach wskazanych przez Zamawiającego (montaż obejmuje wykonanie podłączenia wszystkich urządzeń składowych systemu do sieci zasilającej i teleinformatycznej).

Wykonawca dostarczy wszystkie dodatkowe elementy wyposażenia systemu CCTV IP niezbędne do zamontowania urządzeń i komponentów w miejscach ich instalacji.

Projekt opisuje minimalne wymagania Użytkownika w zakresie technicznym i funkcjonalnym.

Zakłada się, że projektowany system monitoringu CCTV będzie realizowany przy wykorzystaniu serwera NVR, który na tym etapie będzie rejestrować obraz z 3 kamer kopułowych IP (typ1); 7 kamer kopułowych IP (typ2) oraz 1 kamery tubowej IP (typ3). System VMS musi być wyposażony w licencję bazową oraz min 11 licencji na kanał wideo, dodatkowo 1 licencję do zaawansowanej analityki obrazu. Dodatkowo system musi posiadać możliwość integracji interaktywnej zewnętrznej aplikacji internetowej oraz integracji i nagrywania dowolnej interaktywnej aplikacji zewnętrznej. Projektowany system telewizji dozorowej IP zapewni ogląd na żywo i rejestrację wideo z następujących stref:

- a. komunikacja wewnątrz budynku,
- b. teren dookoła obiektu, wejścia/wyjścia z obiektu.

Do nadzoru tych stref użyte zostaną kamery stałopozycyjne wyposażone w obiektywy o ogniskowej zapewniającej pełne pokrycie monitorowanego terenu.

W podziale ogólnym system składał się będzie z:

- a. nowych punktów kamerowych,
- b. przełączników sieciowych PoE,
- c. serwera VMS + dyski do pracy ciągłej,
- d. monitorów do pracy 24/7,
- e. UPS.

Okres przechowywania zapisanego materiału z kamer będzie wynosił co najmniej 30 dni.

Założenia rejestracji:

- a. Kamery wewnętrzne nagrywają stale w strumieniu głównym, z maksymalną rozdzielczością, min 15 kl/s. kodek H.265,
- b. Kamery zewnętrzne nagrywają stale w strumieniu głównym z maksymalną rozdzielczością, min 15 kl/s. kodek H.265.

Wszystkie niezbędne ustalenia związane z punktami kamerowymi i ich zakresem obserwacji, czy też wyświetlaniem poszczególnych kamer na odpowiednich monitorach należy ustalać z Zamawiającym.

Szafy zostaną wyposażone w odpowiednią ilość elementów do zapewnienia prawidłowych połączeń pomiędzy dedykowanymi urządzeniami aktywnymi (switchami) dla systemu monitoringu wizyjnego. Przewidywane jest zainstalowanie kamer

w wskazanych lokalizacjach przedstawionych na planach.

Wszelkie niewymienione w projekcie elementy t.j ustawienia dokładne kąty kamer, maski prywatności należy skoordynować na etapie realizacji. Wszystkie kamery podłączone zostaną do przełączników 1000Mbit z zasilaniem PoE+ znajdujących się w szafie dystrybucyjnej. Miedziane okablowanie poziome punktów CCTV IP służących do transmisji danych ma być prowadzone ekranowanym kablem typu F/FTP (PiMF) kat.6A o paśmie częstotliwościowym 700 MHz, w osłonie bezhalogenowej LSZH-3 zgodna z IEC 60332-3-24(średnica żyły 23AWG). Należy zastosować kabel o klasie odporności na działanie ognia, zgodnie z Euroklasą, minimum B2ca s1 d1 a1.

Wszystkie kamery powinny być oznaczone numerycznie, w sposób trwały. Te same oznaczenia należy umieścić w sposób trwały na gniazdach telekomunikacyjnych na panelach krosowych znajdujących się w każdej Szafie Dystrybucyjnej oraz na każdym urządzeniu końcowym - kamerze.

W DYŻURCE zostanie zainstalowany monitor do pracy ciągłej połączony z GPD.

#### **Zamawiający dopuszcza przed złożeniem oferty przeprowadzenie wizji lokalnej w miejscu wykonania systemu CCTV IP.**

W ramach wykonania systemu CCTV IP należy dokonać:

1. instalacji systemu okablowania strukturalnego miedzianego,
2. budowę tras kablowych wewnątrz i na zewnątrz obiektów,
3. układanie okablowania,
4. budowę punktów dystrybucyjnych,
5. realizację prac wykończeniowych,
6. wykonanie pomiarów linii sygnałowych,
7. instalację i konfigurację 11 kamer (3 wewnętrznych i 8 zewnętrznych), stacji rejestrującej w RAID, minimum 4 dysków twardych w RAID o przestrzeni gwarantującej zapis archiwum minimum 30 dni, zasilacza awaryjnego UPS i szafy typu rak.

Cześć opisowa dotycząca wymagań technicznych i funkcjonalnych systemu CCTV IP:

1. Kamery systemu CCTV IP:
  - a) kamery zewnętrzne Bosch NDE-3503-AL o parametrach wskazanych poniżej:
    - napięcie wejściowe POE 802.3af / 802.3 Type 1, klasa 0 12 VDC  $\pm 30\%$

- typ przetwornika CMOS 1.2/9"
  - obsługa ICR dzień/noc
  - 25 klatek na sekundę przy 4,1 Mpx (2720x1530)
  - kompresja video 265/H;264/H; M-JPEG
  - temperatura pracy -°20 do °50 C,
  - szyfrowanie TLS1.0/1.2,AES128,AES256
  - odporność na uderzenia IK10
  - stopień ochrony przed wodą i kurzem IP66
- b) kamera zewnętrzna Bosch NBE-5503-AL. O parametrach wskazanych poniżej:
- typ przetwornika CMOS 1.2/9"
  - 25 klatek na sekundę przy 4,1 Mpx (2720x1530)
  - szyfrowanie TLS 1.2, SSL, DES, 3DES
  - kompresja video 265/H;264/H; M-JPEG
  - Zasilanie przez PoE (napiecie znamionowe 48 VDC) lub 24 VAC ±10% / +12 VDC ±10%, IEEE 802.3af (802.3at typ 1) Poziom zasilania: klasa 3
  - odporność na uderzenia IK10
  - stopień ochrony przed wodą i kurzem IP67
- c) kamery wewnętrzne Bosch NDV-3503-F02 o parametrach wskazanych poniżej:
- napiecie wejściowe POE IEEE 802.3af / 802.3 at Type 1, klasa 0 12 VDC ±30%
  - typ przetwornika: CMOS 1.2/9"
  - obsługa ICR dzień/noc
  - 25 klatek na sekundę przy rozdzielczości 4,1 Mpx (2720x1530)
  - kompresja video 265/H;264/H; M-JPEG
  - temperatura pracy(ciąglej) -°20 do °50 C
  - szyfrowanie TLS1.0/1.2,AES128,AES256
  - stopień ochrony przed wodą i kurzem IP66
  - kąt widzenia 118° na 69°
2. Stacja rejestrująca z monitorem, zasilaczem awaryjnym UPS i dyskami twardymi:
- a) minimalne wymagane przez Zamawiającego parametry stacji rejestrującej systemu CCTV IP:
- ilość obsługiwanych dysków 4
  - umożliwiające instalację wszystkich wymaganych systemów i archiwów do obsługi CCTV IP
- b) minimalne wymagane przez Zamawiającego parametry monitora przedstawiającego obraz z kamer pracujących w CCTV IP:
- zdolność pracy ciąglej 24/7 (monitor dedykowany do obsługi systemu CCTV IP)
  - 27 cali
  - rozdzielczość ekranu 1920x1080
- c) minimalne wymagane przez Zamawiającego parametry zasilacza awaryjnego UPS:
- moc pozorna 1000VA
  - moc skuteczna 600W
  - czas podtrzymania dla obciążenia 100% - 6 minut
- d) dedykowane dyski twarde do rejestratora minimalne wymagane przez Zamawiającego parametry:
- temperatura pracy od °0 – °65 C

-przeznaczone do pracy ciągłej

3. Szafa rack dedykowana do wyżej wymienionej stacji rejestrującej systemu CCTV IP, zasilacza awaryjnego UPS.

Zamawiający wymaga następujących funkcjonalności systemu:

1. System musi zapewnić możliwość archiwizowania danych (zapis z kamer) przez okres min. 30 dni.
2. Możliwość podglądu obrazu z kamer online jak i zapisów z archiwum systemu w Centrali Najwyższej Izby Kontroli w Warszawie przy ulicy Filtrowej 57.

Wymagania funkcjonalne dla oprogramowania do zarządzania systemem CCTV IP:

1. Zamawiający wymaga dostarczyć oprogramowanie do systemu wraz z dożywotnią licencją przeznaczone do zdalnego zarządzania, konfiguracji i administrowania systemem CCTV IP, licencja musi umożliwiać używanie dowolnych składników ww. oprogramowania na dowolnej liczbie stanowisk komputerowych – licencja oprogramowania na klienta.
2. Interfejs oprogramowania musi być dostępny w polskiej wersji językowej.
3. Zamawiający wymaga aby oprogramowanie posiadało możliwość wykonania okresowej kopii zapasowej bazy danych na wskazany udział sieciowy (przestrzeń dyskowa udostępniona przez Zamawiającego).
4. Oprogramowanie musi zapewniać możliwość zdalnego zarządzania systemem CCTV IP poprzez sieć Ethernet z wykorzystaniem protokołu TCP/IP.
5. Oprogramowanie musi zapewniać zdalne monitorowanie stanu systemu CCTV IP.
6. Zamawiający wymaga dokonać instalacji i konfiguracji ww. oprogramowania w miejscu wskazanym przez zamawiającego dla administratora i personelu obsługi.
7. Zamawiający wymaga od wykonawcy w ramach usług wsparcia technicznego by zapewnił przynajmniej raz na rok aktualizację (w trybie OFFLINE bez konieczności podłączania urządzenia do sieci Internet) oprogramowania do najnowszej obowiązującej wersji.
8. System CCTV IP musi posiadać wbudowany zegar czasu rzeczywistego pracujący również po wyłączeniu zasilania głównego i zasilania awaryjnego oraz umożliwiać ustawienie synchronizacji czasu z serwera zewnętrznego w oparciu o protokół NTP.
9. Oprogramowanie musi zapewniać tworzenie grup użytkowników ( personel obsługi systemu) w celu sprawnego i efektywnego zarządzania systemem co najmniej dla:
  - a) grup administratorów systemu z podziałem na różne zakresy kompetencji,
  - b) grupy pracowników ochrony mających wgląd do raportów i rejestrów,
  - c) uwierzytelnienie użytkowników w oprogramowaniu do zarządzania system CCTV IP powinno odbywać się po wprowadzeniu indywidualnego loginu oraz hasła składającego się z min. 8 znaków – cyfr i znaków alfanumerycznych z możliwością ustawienia w systemie okresu wymuszania zmiany hasła dla użytkowników,
  - d) wymuszenie przez system okresowej zmiany hasła w systemie dla konta administratora,
  - e) możliwość odczytania daty założenia konta użytkownika w systemie,
  - f) możliwość odczytania kto (jaki użytkownik) założył dane konto w systemie,
  - g) możliwość wygenerowania raportu dla danego użytkownika systemu zawierającego: wszystkie dane dotyczące jego konta w systemie tj. imię, nazwisko itp. Oraz dodatkowo informację z pkt. e,f.
10. Umożliwić ustawienie blokady konta użytkownika np. urlop pracownika, zwolnienie z pracy.

## 11. Platform Software Development Kit (SDK):

a) VMS musi obsługiwać zestaw do opracowywania oprogramowania (SDK), który umożliwia integrację systemu zarządzania za pomocą sygnału wizyjnego z aplikacjami innych firm, na przykład kontrolą dostępu i analityką wideo.

b) Typy i funkcje integracji: Integracja aplikacji i wtyczek stron trzecich jest możliwa na trzy różne sposoby:

1. Integracja przez protokoły sieciowe powinna umożliwiać wybór platformy kodowania. Integracja za pomocą protokołów powinna zapewniać:

- a) Pobieranie, zapisywanie i zmianę konfiguracji systemu VMS.
- b) Pobieranie bieżącego lub nagranego obrazu wideo, dźwięku i metadanych.
- c) Wysyłanie poleceń sterujących i zdarzeń do systemu VMS.
- d) Odbieranie informacji o stanie systemu VMS, na przykład o awarii kamery lub wyczerpaniu miejsca na serwerze.
- e) Wdrażanie protokołów w systemach Windows, Java® i Linux®.

2. Integracja przez biblioteki .NET, które umożliwiają wykorzystanie komponentów oprogramowania do integracji z systemem VMS. Integracja .NET powinna zapewniać:

- a) Pobieranie, zapisywanie i zmianę konfiguracji systemu VMS.
- b) Pobieranie bieżącego i nagranego dźwięku oraz metadanych.
- c) Wyświetlanie bieżącego i zarejestrowanego obrazu wideo z opcjonalną nakładką graficzną.
- d) Wydawanie poleceń sterujących do systemu VMS lub powiązanego urządzenia, na przykład kamery z funkcjami PTZ i wyjściami.
- f) Wysyłanie i odbieranie zdarzeń w ramach systemu VMS.

3. Integracja przez wtyczkę osadzoną bezpośrednio w środowisku VMS, która powinna działać jako część VMS i aplikacji klienckich. Integracja za pomocą wtyczki powinna zapewniać:

- a) Zintegrowanie z serwerem zdarzeń, umożliwiając serwerowi zdarzeń korzystanie z funkcji wtyczki. Umożliwia to realizację funkcji opartych na zdarzeniach bez potrzeby korzystania z otwartego interfejsu użytkownika.
- b) Zintegrowanie z Smart Client, co umożliwia aplikacji korzystanie z funkcjonalności wtyczek.
- c) Zintegrowanie z Management Client, co umożliwia aplikacji korzystanie z funkcjonalności wtyczek.
- d) Wtyczki muszą działać we wszystkich produktach i wersjach VMS.
- e) Wtyczki muszą mieć możliwość nasłuchiwania zdarzeń z innych wtyczek.
- f) Powinno być możliwe aktywowanie licencji dla wtyczek stron trzecich w Management Client.

c) Możliwości integracji: Aplikacje stron trzecich muszą mieć możliwość integracji z VMS w celu uzyskania dostępu do różnych funkcji:

1. Funkcje wideo, dźwięku i metadanych:

- a) Pobieranie i odtwarzanie bieżących i nagranych materiałów wideo.

- b) Pobieranie i odtwarzanie bieżących i nagranych materiałów audio.
  - c) Pobieranie i dostęp do metadanych bieżących i zapisanych.
  - d) Pobieranie i wyświetlanie pojedynczych obrazów (JPEG).
  - e) Eksportowanie obrazu wideo i dźwięku w formatach AVI, MKV i natywnym formacie bazy danych.
  - f) Umieszczanie informacji o nakładkach na obrazie wideo przekazywanym na żywo, jak i na obrazie zarejestrowanym w implementacji opartej na komponentach oraz we wtyczkach dla Smart Client.
  - g) Tworzenie, znajdowanie i usuwanie zakładek.
2. Konfiguracja:
- a) Odzyskiwanie i zmiana konfiguracji VMS, w tym informacji o kamerach, użytkownikach i alarmach.
  - b) Umożliwienie aplikacjom firm trzecich zapisywania i pobierania własnej konfiguracji.
3. Uwierzytelnianie i autoryzacja. Logowanie i autoryzacja wtyczek, aplikacji i integracji protokołów stron trzecich:
- a) Zarządzanie uprawnieniami użytkowników do funkcjonalności wtyczek.
  - b) Ramy dla dostępu do systemu i obsługi tokenów bezpieczeństwa.
4. Zdarzenia i alarmy:
- a) Wyzwalanie wewnętrznych (związanych z systemem) i zewnętrznych (zintegrowanych) zdarzeń i alarmów.
  - b) Określone zdarzenie może spowodować rozpoczęcie lub zatrzymanie nagrywania.
  - c) Wyszukiwanie istniejących alarmów i zdarzeń.
  - d) Aktualizacja i potwierdzanie alarmów.
5. Licencjonowanie. Należy przeczytać licencje i dodać własną licencję wtyczki:
- a) Licencjonowanie integracji firm trzecich.
  - b) Integracja z rejestracją online.
6. Status systemu:
- a) Odbieranie wszystkich komunikatów o statusie systemu VMS, włączając w to dyski serwera, wykorzystanie procesora i wyzwalane zdarzenia.
7. Sterowanie. Wyzwalanie wyjścia, sterowanie obrotem/pochyleniem/powiększeniem, uruchamianie/zatrzymywanie nagrań:
- a) Wysyłanie poleceń PTZ do kamer.
  - b) Pobieranie pozycji PTZ z bezwzględnych kamer PTZ.
  - c) Wysyłanie zdarzeń rozpoczęcia lub zatrzymania nagrywania z określonego zdarzenia.
  - d) Ustawianie zakładek podczas nagrywania.
  - e) Aktywacja wyjścia zewnętrznego.
  - f) Sterowanie funkcjonalnością aplikacji do obsługi ściany wideo.
  - g) Wysłanie kamery do monitora udostępniającego wideo.

- h) Wysyłanie poleceń do wtyczek opracowanych przez inne firmy.
  - i) Kontroler czasu odtwarzania.
  - j) Wsparcie dla wyświetlania elementów wtyczki na inteligentnej mapie w aplikacji Smart Client.
  - k) Zmiana motywu Smart Client.
8. Dzienniki systemu i inspekcji. Generowanie wpisów do dzienników i odczytywanie dzienników:
- a) Zapisywanie i odczytywanie dzienników systemowych i dzienników inspekcji.
12. Kontrola i bezpieczeństwo informacji: Należy zapewnić następujące środki ochrony danych i możliwości zarządzania prawami użytkowników w celu wspierania poufności, integralności i dostępności systemu:
- 1) Dane w tranzycie: Szyfrowana komunikacja pomiędzy serwerami i klientami z wykorzystaniem bezpiecznych certyfikatów cyfrowych CA.
    - a) Połączenia HTTPS z serwera rejestrującego do urządzeń, które obsługują połączenia HTTPS.
    - b) Szyfrowana komunikacja pomiędzy serwerem rejestrującym a usługami odzyskującymi dane strumieniowe z wykorzystaniem dostarczonych przez klienta certyfikatów cyfrowych CA dla połączeń z serwerem rejestrującym.
    - c) Szyfrowana komunikacja między serwerem zarządzającym a serwerem rejestrującym przy użyciu certyfikatów cyfrowych CA dostarczonych przez klienta.
    - d) Połączenia HTTPS z klientów VMS, klientów SDK oraz usług, które obsługują połączenia HTTPS, do serwera rejestrującego.
  - 2) Dane konfiguracji systemu: Należy zapewnić ochronę hasłem kopii zapasowej konfiguracji systemu.
  - 3) Transmisja nagrań wideo na żywo i w czasie rzeczywistym poza lokalizacją: Połączenia HTTPS muszą używać zaufanych certyfikatów CA i obsługiwać połączenia HTTPS z:
    - a) Serwera usług mobilnych do opartych na przeglądarce aplikacji XProtect Web Client i klienta XProtect Mobile.
    - b) Aplikacji Open Network Bridge do zdalnych systemów publicznych.
  - 4) Integralność danych eksportowanego materiału wideo:
    - a) Eksportowanie wideo w formacie, który może być oglądany tylko w aplikacji Smart Client - Player.
    - b) Ochrona hasłem przy odtwarzaniu dla każdego eksportu.
    - c) 256-bitowe szyfrowanie AES.
    - d) Cyfrowe podpisywanie wyeksportowanych mediów algorytmem SHA-2 w celu ustanowienia sposobu wykrywania modyfikacji wyeksportowanego wideo.
    - e) Należy zapewnić funkcję weryfikacji podpisów w odtwarzaczu Smart Client - Player do uwierzytelniania autentyczności eksportowanego nagrania wideo.
    - f) Należy zapewnić opcję zapobiegającą ponownemu eksportowi wyeksportowanego wideo.
  - 5) Certyfikaty cyfrowe: Wykorzystanie certyfikatów cyfrowych CA dostarczonych przez klienta do połączeń z serwerem usług mobilnych.
  - 6) Kontrola dostępu do danych: Należy zapewnić:

- a) Profile użytkowników ograniczające dostęp do urządzenia oraz przeglądanie, odtwarzanie i eksportowanie wideo, w tym według dnia i pory dnia.
  - b) Dziennik inspekcji ze znacznikami czasowymi informujący o tym, kto się zalogował, oglądał obraz na żywo lub nagrany, albo wyeksportował obraz wideo.
13. Zaawansowana analiza wideo: zaawansowane, dodatkowe rozwiązanie do analiz wideo prowadzonych w celach kryminalistycznych, za pomocą którego możesz szybko przeglądać i analizować treści video, aby sprawnie znaleźć to, czego szukasz.
- 1) VIDEO SYNOPSIS®: Rozwiązanie VIDEO SYNOPSIS zapewnia jednoczesną prezentację obiektów, które pojawiły się na wideo o różnym czasie. Zapewnia to znaczne skrócenie segmentu wideo wraz z zachowaniem możliwości analizy sceny przez oglądającego, dzięki czemu wielogodzinne wideo można przeglądać w ciągu kilku minut, a czasami sekund.
  - 2) Zarządzanie przypadkami: Uporządkuj wszystkie zasoby wideo w jednym kontenerze, dodaj do zakładki interesujące Cię obiekty oraz podsumuj wnioski (w tym wszystkie odpowiednie dowody), tworząc raport, który można wyeksportować, i jednocześnie prowadząc dynamiczną współpracę w zakresie przypadków z innymi użytkownikami.
  - 3) Wyszukiwanie obejmujące wiele kamer: Potężne i zaawansowane możliwości wyszukiwania w wielu kamerach dla wszystkich filtrów wyszukiwania i warstw wizualnych.
  - 4) Identyfikacja odległości: Wyszukiwanie i określanie odległości między osobami w czasie i lokalizacji w celu przestrzegania dystansu fizycznego oraz śledzenia kontaktów, jak również w przypadku dochodzeń w sprawach karnych.
  - 5) Wykrywanie maseczek: Przeszukiwanie i filtrowanie nagrań wideo w celu identyfikacji użycia maseczek.
  - 6) Rozpoznawanie twarzy: Dokładne rozpoznawanie twarzy w celu szybkiego wskazywania osób umieszczonych lub wykluczonych z listy obserwowanych na podstawie obrazów pobranych z istniejących nagrań wideo lub przesłanych danych.
  - 7) Rozpoznawanie tablic rejestracyjnych: Zróżnicowane rozpoznawanie tablic rejestracyjnych przeznaczone specjalnie do nadzoru „w naturalnym środowisku” oraz ułatwiania pracy podczas wyszukiwania tablic rejestracyjnych na listach obserwacyjnych, w istniejącym wideo lub przesyłanych danych.
  - 8) Przekraczanie linii: Wykrywanie, filtrowanie i liczenie obiektów przekraczających linię graniczną w określonym kierunku w celu stymulowania ochrony obwodowej oraz zliczania obiektów poruszających się w danym kierunku.
  - 9) Podobieństwo wyglądu: Natychmiastowe lokalizowanie ludzi, pojazdów i innych przedmiotów, którymi jesteśmy zainteresowani, dzięki możliwości wyszukiwania obiektów o podobnych atrybutach.
  - 10) Warstwy wizualne: Tworzenie analiz wizualnych w zakresie aktywności, czasu przebywania, często wykorzystywanych ścieżek i zmian tła.
  - 11) Tolerancja filtra: Dostosowanie poziomów tolerancji, aby doprecyzować wyniki wyszukiwania.
  - 12) Kontrola gęstości i szybkości: Zwiększanie lub zmniejszanie liczby i szybkości zdarzeń, które są przedstawiane w tym samym czasie.
  - 13) Kontrola sortowania: Wyświetlanie zdarzeń według ich odpowiedniości lub kolejności, w jakiej wystąpiły, oraz łatwe powiększanie interesujących nas elementów.

#### Dokumentacja powykonawcza systemu CCTV IP:

1. Wykonawca najpóźniej w dniu odbioru zleconych prac przekaze Zamawiającemu dokumentację powykonawczą uwzględniając poniższe zagadnienia:
  - a) Rzuty budynków uwzględniające umiejscowienie elementów systemu podlegających dostawie i instalacji oraz przebieg tras kablowych i miejsce przyłączenia składowych systemu do sieci energetycznej,
  - b) Sposób podłączenia zasilania elektrycznego ( tablica elektryczna, nr obwodu, zabezpieczenia nadprądowe i różnicoprądowe )
  - c) Adresację sieci Ethernet protokołu TCP/IP,
  - d) Trasy i sposób ułożenia przewodów,
  - e) Kartę gwarancyjną dla dostarczonych składowych systemu CCTV IP,
  - f) Protokół pomiarów elektrycznych ochrony przeciwpożarowej dla zainstalowanych urządzeń (metalowe obudowy urządzeń),
  - g) Dokument potwierdzający uprawnienia do korzystania z licencji na oprogramowanie,
  - h) Dokumentacja w formacie PDF na płycie DVD lub pendrive USB i w trzech egzemplarzach w wersji papierowej z załączonym oświadczeniem o zgodności montażu z obowiązującymi przepisami.
2. Dostarczenie instrukcji obsługi dla użytkowników systemu z zakresu codziennej obsługi systemu w wersji papierowej ( w 3 egzemplarzach ) i elektronicznej ( w formacie PDF, na płycie DVD lub pendrive USB ).
3. Dostarczenie instrukcji obsługi, funkcjonowania i konserwacji dla administratora systemu z ujętymi procedurami postępowania w sytuacjach awaryjnych w wersji papierowej (w 3 egzemplarzach) i elektronicznej ( w formacie PDF, na płycie DVD lub pendrive USB ).
4. Urządzenia – składowe systemu muszą posiadać deklarację zgodności CE wydaną przez producenta w języku polskim lub tłumaczenie (w formie kopii potwierdzonej za zgodność z oryginałem)  
lub oświadczenie Wykonawcy, że oferowane urządzenie spełnia wymogi normy CE i posiada znak CE (w oryginale ).

#### Wymagania gwarancyjne i wsparcie techniczne dla systemu CCTV IP:

1. Wykonawca zapewni na dostarczone urządzenia minimalną 24 – miesięczną gwarancję producenta (chyba, że producent stanowi inaczej) obowiązującą od dnia podpisania Protokołu odbioru przedmiotu Umowy.
2. Na wykonany przedmiot umowy inny niż wskazany w ust. 1 Wykonawca udzieli Zamawiającemu 24 miesięcznej gwarancji liczonej od dnia podpisania Protokołu odbioru przedmiotu Umowy.
3. Gwarancja będzie obejmować:
  - a) usługi napraw urządzeń,
  - b) usunięcie usterek spowodowane wadliwymi częściami i/lub defektami produkcyjnymi usterki uniemożliwiającymi prawidłowe działanie systemu,
  - c) naprawę elementów podlegających normalnemu zużyciu podczas eksploatacji,
  - d) koszty transportu,
  - e) możliwość zgłaszania awarii 24h/dobę.
4. W uzasadnionych przypadkach dopuszcza się możliwość zdalnego świadczenia usług w ramach gwarancji.
5. Reakcja serwisu Wykonawcy na awarię nie może być dłuższa niż w ciągu 8 godzin w dni robocze liczone od momentu dokonania zgłoszenia wystąpienia awarii.

6. Czas naprawy nie przekroczy 24 godzin w dni robocze Zamawiającego, licząc od chwili zgłoszenia przez Zamawiającego, z możliwością przedłużenia w uzasadnionych przypadkach do 7 dni roboczych, po uprzednim uzyskaniu zgody Zamawiającego.
7. Wykonawca zapewni wsparcie techniczne przez okres trwania gwarancji obejmującej:
  - a) Przegląd gwarancyjny w lokalizacjach instalacji urządzeń (w 10 i 22 miesiącu obowiązywania gwarancji) obejmujący m.in. ścieżkę diagnostyczną, regulację i czyszczenie elementów, wymianę zużytych bądź uszkodzonych elementów,
  - b) Zdalne i telefoniczne konsultacje techniczne w zakresie eksploatacji urządzeń i oprogramowania, w dniach roboczych, w godz. 8-16.

### **Wymagania dotyczące montażu oraz uruchomienia:**

#### **Podstawowe zasady w ramach wykonywania instalacji:**

- 1) Stosować sprawne narzędzia, sprzęt, aparaturę, materiały i urządzenia posiadające aktualne świadectwa dopuszczenia, atesty i certyfikaty.
- 2) Pracownicy Wykonawcy muszą być przeszkoleni pod kątem BHP.
- 3) Kable powinny być układane w temperaturach określonych przez ich producenta (z reguły od -50C do +50C).
- 4) Promień gięcia kabla nie powinien być mniejszy niż określony przez producenta i podany w odpowiedniej normie.
- 5) Zachować odstępy od innych instalacji określone w odpowiednich normach.
- 6) Przejścia przez ściany i stropy wykonywać z użyciem rur (po wciągnięciu kabli, zwłaszcza na granicach stref pożarowych wykonać uszczelnienia przy użyciu certyfikowanych mas ppoż.).
- 7) W celu rozprowadzenia przewodów zastosować rurki elektroinstalacyjne, peszle, metalowe koryta kablowe.
- 8) Zaleca się wciągnięcie drutu stalowego („pilotów”) do rurek w celu ułatwienia wprowadzania przewodów (przepusty).
- 9) Ciągi instalacji należy umieszczać poniżej instalacji elektroenergetycznych.

#### **Zasady obowiązujące przy budowie tras kablowych i układaniu kabli:**

- 1) Trasy kablowe należy zbudować z elementów trwałych pozwalających na zachowanie odpowiednich promieni gięcia wiązek kablowych na zakrętach (wartości minimalnych promieni gięcia kabli są podane w kartach katalogowych kabli miedzianych i światłowodowych).
- 2) Rozmiary (pojemność) kanałów kablowych należy dobierać w zależności od maksymalnej liczby kabli projektowanych w danym miejscu instalacji (należy przyjąć zapas 20% na potrzeby ewentualnej rozbudowy systemu).
- 3) Zajątość światła kanałów kablowych przez kable należy obliczać w miejscach zakrętów kanałów kablowych. Przy całkowitym wypełnieniu światła kanału kablami na zakręcie kanał będzie wówczas wypełniony w 40% na prostym odcinku. Przy budowie tras kablowych pod potrzeby okablowania strukturalnego należy wziąć pod uwagę zapisy normy 50174-2:2010/A1:2011 dotyczące równoległego prowadzenia różnych instalacji w budynku, m.in. instalacji zasilającej, zachowując odpowiednie odległości pomiędzy okablowaniem zasilającym, a okablowaniem strukturalnym przy jednoczesnym uwzględnieniu materiału, z którego zbudowane są kanały kablowe.
- 4) Przy układaniu kabli, zarówno miedzianych, jak i światłowodowych należy stosować się do odpowiednich zaleceń producenta (tj. promienia gięcia, siły i sposobu wciągania, itp.). Symetryczne kable skrętakowe należy układać w wybudowanych kanałach kablowych w sposób odpowiadający odporności konstrukcji kabla na wszelkie uszkodzenia mechaniczne. W szczególności należy wystrzegać się nadmiernego ściskania kabli, deptania po kablach ułożonych na podłodze oraz załamывania kabli na elementach konstrukcji kanałów kablowych. Przy odwijaniu kabla z bębna bądź wyciąganiu kabla z pudełka nie należy przekraczać maksymalnej siły ciągnięcia oraz zwracać uwagę na to, by na kablu nie tworzyły się węzły ani supły. Przyjęty ogólnie promień gięcia podczas

instalacji wynosi 8 krotność średnicy zewnętrznej kabla skrętkowego. Kable światłowodowe przeznaczone do instalacji wewnątrz budynków są szczególnie narażone na ściskanie, zgniatanie oraz załamywanie,

dlatego podczas układania czy wciągania kabli światłowodowych należy zwrócić szczególną uwagę na to by tych kabli nie deptać, zagniatć i załamywać. Prawidłowy proces wciągania kabli światłowodowych wymaga chwytu za kevlar lub inne elementy zabezpieczające włókna (np. włókna aramidowe, pręty GRP), a nie za zewnętrzną osłonę kabla, która użyta do chwytu celem wciągania, może ulec uszkodzeniu lub osłabieniu. Przy prowadzeniu kabli w kanałach kablowych należy różne rodzaje kabli układać w oddzielnych przegrodach kanału. Jeśli brak takiej możliwości, kable światłowodowe powinny być układane na wierzchu.

- 5) Przy układaniu kabli na styku (skrzyżowania i zbliżenia) z innymi instalacjami należy stosować odcinki rurek lub inne przekładki izolacyjne.
- 6) Należy koordynować przebieg tras kabli danej instalacji oraz innych instalacji.
- 7) Nie wykonywać żadnych połączeń przewodów poza tymi, które wskazuje projekt.
- 8) Nie wolno wykonywać nadmiarowych połączeń przewodów.

#### Zasady obowiązujące przy budowie punktów dystrybucyjnych:

- 1) Elementy punktów dystrybucyjnych powinny być umieszczane w szafach dystrybucyjnych stanowiących zabezpieczenie pasywnych paneli krosowych, urządzeń aktywnych, kabli elastycznych oraz innego instalowanego w stelażu sprzętu.
- 2) Minimalna odległość pomiędzy ścianą boczną szafy, a ścianą pomieszczenia powinna wynosić 15 cm.
- 3) Zaleca się prowadzenie oddzielnych wiązek kablowych do poszczególnych paneli krosowych.
- 4) Należy stosować zapas kabli wewnątrz szafy umożliwiający umieszczenie panela w dowolnym miejscu stelażu.
- 5) Do umocowania wiązek kablowych należy wykorzystać elementy montażowe szafy. Przy mocowaniu wiązek kablowych należy przestrzegać zasad maksymalnej siły ściskania kabla, zależnej od jego konstrukcji, podawanej w kartach katalogowych produktów. Wszystkie ekranowane panele krosowe wymagające doprowadzenia potencjału uziomu budynku są wyposażone w odpowiedni zacisk. Należy doprowadzić do nich przewód giętki (linkę) w izolacji żółtozielonej, zakończyć ją na wspólnej szynie uziemiającej szafy.

#### Zasady dotyczące terminowania kabli w osprzęcie przyłączeniowym:

- 1) Do terminowania końcówek kabli w osprzęcie przyłączeniowym należy stosować odpowiednie narzędzia przygotowane do konkretnego rodzaju kabla.
- 2) Należy przestrzegać zapisów instrukcji montażu osprzętu połączeniowego w odniesieniu do zdejmowania koszulki zewnętrznej kabla, rozplotu elementów ekranujących oraz rozkręcania poszczególnych par (działania te mają bezpośredni wpływ na wydajność toru transmisyjnego).

#### Zasady dotyczące trasowania:

- 1) Trasa instalacji okablowania strukturalnego powinna przebiegać bezkolizyjnie z innymi instalacjami i urządzeniami.
- 2) powinna być przejrzysta, prosta i dostępna dla prawidłowej konserwacji oraz remontów.
- 3) W przypadku długich traktów, gdzie kable sieci teleinformatycznej i zasilającej biegną równolegle do siebie na odległości większej niż 35 m, należy zachować odległość między instalacjami, co najmniej 50 mm. Minimalna odległość między kablami informatycznymi i lampami fluoroscencyjnymi, neonowymi i próżniowo-lukowymi (lub innymi o wysokim poziomie prądu rozładowania) powinna wynosić 130 mm. Kable stosowane w różnych celach (np. zasilające energią elektryczną i informatyczne) nie powinny być umieszczane w tych samych wiązkach. Różne wiązki powinny być oddzielone elektromagnetycznie od siebie. Szczegółowe informacje w

Zasady dotyczące montażu konstrukcji wsporczych oraz uchwytów:

- 1) Konstrukcje wsporcze i uchwyty przewidziane do ułożenia na nich instalacji okablowania strukturalnego bez względu na rodzaj instalacji, powinny być zamocowane do podłoża w sposób trwały, uwzględniający warunki lokalne i technologiczne, w jakich dana instalacja będzie pracować, oraz sam rodzaj instalacji.

Zasady prowadzenia instalacji przez ściany i stropy:

- 1) Wszystkie przejścia obwodów instalacji okablowania strukturalnego przez ściany i stropy itp. muszą być chronione przed uszkodzeniami.
- 2) Przejścia te należy wykonywać w przepustach rurowych.
- 3) Obwody instalacji okablowania strukturalnego przechodząc przez podłogi muszą być chronione do wysokości bezpiecznej przed przypadkowymi uszkodzeniami.
- 4) Jako osłony przed przypadkowymi uszkodzeniami mechanicznymi należy stosować rury stalowe, rury z tworzyw sztucznych, korytka blaszane itp.

Weryfikacja systemów ( okablowanie, komponenty ):

- 1) Weryfikacja struktury systemu okablowania będzie polegała na sprawdzeniu rozplanowania elementów okablowania w budynku bądź budynkach oraz długości połączeń pomiędzy nimi. Muszą być spełnione wymagania opisane w PN-EN 50173-1:2011.
- 2) Weryfikacja doboru komponentów - zgodnie z normą PN-EN 50173-1:2011 wydajność systemu okablowania definiują komponenty składające się na poszczególne tory transmisyjne. Kable i połączenia różnych kategorii mogą być mieszane ze sobą w kanale, jednakże o wydajności kanału będzie decydował element o najsłabszej wydajności. W przypadku doboru komponentów światłowodowych muszą być spełnione zapisy tej samej normy PN-EN 50173-1:2011.
- 3) Weryfikacja wydajności systemu okablowania - sprawdzenie wydajności systemu okablowania w rozumieniu poszczególnych jego łączy stałych bądź kanałów będzie polegała na przeprowadzeniu badań wydajności zgodnie z normą EN 50346:2004/A2:2010 z zastosowaniem odpowiednich przyrządów określonej dokładności. Należy przeprowadzić badania wydajności łączy stałych okablowania poziomego w klasie wydajności, w jakiej projektowano i wykonywano system okablowania. Wynik badań powinien być pozytywny dla wszystkich łączy stałych systemu.
- 4) Weryfikacja jakości wykonania prac wykończeniowych będzie polegała na wizualnym sprawdzeniu wszelkich prac wykończeniowych, włączając w to sprawdzenie zgodności dokumentacji powykonawczej ze stanem rzeczywistym instalacji.

Prace wykończeniowe:

Należy zamknąć wszelkie otwory rewizyjne wykorzystywane podczas instalacji kabli. Jeśli wykorzystuje się trasę kablową przechodzącą przez granicę strefy pożarowej, światło jej otworu należy zamknąć odpowiednią masą uszczelniającą, charakteryzującą się właściwościami nie gorszymi niż granica strefy, zgodnie z przepisami p.poż. i przymocować w miejscu jej instalacji przywieszkę z pełną informacją o tak zbudowanej granicy strefy. Należy oznaczyć wszystkie zainstalowane elementy zgodnie z zasadami administrowania systemem okablowania, wykorzystując opracowany wcześniej otwarty system oznaczeń, pozwalający na późniejszą rozbudowę instalacji. Elementami, które należy oznaczać są:

- a. pomieszczenia punktów dystrybucyjnych,

- b. szafy zawierające elementy systemu okablowania,
- c. poszczególne panele krosowe,
- d. poszczególne porty tych paneli,
- e. wszystkie gniazda użytkowników.

Oznaczenia powinny być trwałe, wyraźne i widoczne. Po zakończeniu instalacji należy przygotować dokumentację powykonawczą zawierającą następujące elementy:

- a. podstawa opracowania,
- b. informacje o inwestorze,
- c. opis wykonanej instalacji wraz z zainstalowanym opisem wybranej technologii,
- d. lista zainstalowanych komponentów: Lp. / Producent –Dostawca / Numer katalogowy / Nazwa elementu / Ilość
- e. schemat połączeń elementów instalacji,
- f. widoki szaf w punktach dystrybucyjnych,
- g. widoki wszystkich rodzajów punktów użytkowników.

#### Sprawdzenie instalacji:

Po zakończeniu robót, a przed oddaniem instalacji do eksploatacji należy przeprowadzić sprawdzenie odbiorcze zgodnie z PN-IEC 60364-6-61:2000. Włączenie zasilania urządzeń systemów teletechnicznych musi być dokonane (po zakończeniu prac związanych z ich montażem i wstępnym sprawdzeniem –wg procedur określonych poniżej) przy udziale wykonawcy branży elektrycznej. Po włączeniu zasilania należy pomierzyć napięcia i/lub wartości rezystancji uziemień na zaciskach ogółu urządzeń systemów teletechnicznych zasilanych z sieci 230V 50Hz. Należy opracować protokół z badań i pomiarów, który powinien być przedstawiony później komisji odbioru robót.

#### Uruchomienie systemu CCTV IP:

1. Do urządzenia należy doprowadzić zasilanie z wydzielonych obwodów sieci energetycznej (z najbliższej rozdzielni elektrycznej ) z własnym zabezpieczeniem minimum nadprądowym.
2. Uruchomienie systemu oraz wykonanie wstępnej konfiguracji kamer w oparciu o zestaw danych dostarczony przez Zamawiającego.
3. Instruktaż obsługi systemu CCTV IP dla osób zarządzających po stronie Zamawiającego w zakresie zarządzania oraz obsługi systemu Wykonawca zrealizuje w lokalizacjach instalacji dla grupy 7 osób w ciągu 2 dni od dnia odbioru prac.
4. Przeprowadzi testy prawidłowego działania elementów składowych systemu, funkcjonalności oprogramowania stosowania przykładowo nadanych uprawnień.

#### Odbiór robót:

Z czynności odbioru zostanie sporządzony protokół odbioru przedmiotu Umowy, którego wzór stanowi **Załącznik nr 4** do Umowy.

Czynności odbioru systemu wykonuje komisja w składzie:

- a. przedstawiciel Zamawiającego,
- b. Inspektor nadzoru ze strony Zamawiającego,
- c. Przedstawiciel Wykonawcy.

