

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Określenie przedmiotu i zakresu zamówienia:

Przedmiotem zamówienia jest dostawa urządzeń, rozbudowa i modernizacja systemu Monitoringu Prewencyjnego Wrocławia z wykorzystaniem infrastruktury systemu łączności radiowej typu LMDS.

2. Wymagania ogólne:

- 2.1. Zamawiający wymaga, aby zamówienie było zrealizowane kompletnie, w pełnym zakresie i zgodnie z wymaganiami Zamawiającego określonymi w niniejszym OPZ, SWZ oraz warunkami umowy.
- 2.2. Zamawiający wymaga, aby zamówienie było wykonane z należytą starannością, w oparciu o sprawdzone, nowoczesne technologie, z wykorzystaniem współczesnej wiedzy z zakresu związanego z przedmiotem zamówienia, z poszanowaniem wszelkich obowiązujących przepisów prawa.
- 2.3. Zamawiający wymaga, aby oferowane przez Wykonawcę urządzenia były jednorodne (tj. zakazuje się zaoferowania a następnie dostarczania różnych modeli urządzeń, urządzenia muszą być tożsame w ramach modelu).
- 2.4. Ze względu na konieczność dostarczenia rozwiązań kompatybilnych względem siebie, Zamawiający wymaga, aby wszystkie dostarczane akcesoria oraz osprzęt pochodziły z katalogu akcesoriów dedykowanych dla oferowanego modelu urządzenia. Wykonawca jest zobowiązany dostarczyć stosowne dokumenty potwierdzające kompatybilność rozwiązań technicznych w przypadku, gdy oferowane elementy pochodzą od innego producenta niż producent tego urządzenia.

- 2.5. Wszystkie oferowane urządzenia, sprzęt i akcesoria muszą być ogólnodostępne na rynku, tzn. być produkowane seryjnie i znajdować się w aktualnej ofercie ich producentów.
- 2.6. Zamawiający wymaga aby kamery sieciowe oraz głośniki sieciowe były kompatybilne z systemem Monitoringu Prewencyjnego Wrocławia pracującym w oparciu o zintegrowaną platformę bezpieczeństwa Genetec Security Center. Aktualna lista urządzeń kompatybilnych z przedmiotowym systemem znajduje się na stronie internetowej:
<https://www.genetec.com/supported-device-list>
- 2.7. Zamawiający wymaga, aby wszystkie urządzenia sieciowe (w szczególności kamery oraz przełączniki sieciowe) posiadały wbudowany interfejs konfiguracyjny dostępny z poziomu przeglądarki www (Chrome, Firefox, Opera) bez konieczności instalacji dodatkowego oprogramowania lub sterowników.
- 2.8. Zgodnie z Prawem Zamówień Publicznych zezwala się na dobór urządzeń równoważnych względem urządzeń wskazanych w treści niniejszego dokumentu jako modele przykładowe (referencyjne) o parametrach nie gorszych niż przedstawionych w OPZ. Na etapie składania ofert Wykonawca zobowiązany jest oświadczyć, że oferowane dostawy i usługi odpowiadają wymaganiom określonym przez Zamawiającego.

3. Wymagania ilościowe:

Wykonawca zobowiązany jest:

- 3.1. Wybudować i uruchomić kompleksową instalację monitoringu obejmującą Podwórko Wszystkich Mieszkańców zlokalizowane w kwartale ulic Komuny Paryskiej, Miernicza, Łukasińskiego, Prądyńskiego we Wrocławiu.
- 3.2. Wybudować i uruchomić kompleksową instalację monitoringu obejmującą wnętrze podwórzowe przy ulicy Kościuszki 35a we Wrocławiu.

- 3.3. Wybudować i uruchomić kompleksową instalację monitoringu obejmującą wnętrze podwórzowe przy ulicy Podwale 74 we Wrocławiu.
- 3.4. Wybudować i uruchomić kompleksową instalację monitoringu obejmującą tereny przyległe do budynku przy ulicy Góralskiej 38 we Wrocławiu.
- 3.5. Wybudować i uruchomić kompleksową instalację monitoringu obejmującą skrzyżowanie ulicy Kolejowej z placem Rozjezdnym we Wrocławiu.
- 3.6. Wybudować i uruchomić kompleksową instalację monitoringu obejmującą skrzyżowanie ulicy Bystrzyckiej i Metalowców we Wrocławiu.
- 3.7. Wybudować i uruchomić kompleksową instalację monitoringu obejmującą tereny przyległe do Jazu Małgorzata we Wrocławiu.
- 3.8. Wybudować i uruchomić łącze radiowe LMDS na potrzeby punktu kamerowego przy ulicy Wielkopolskiej 16 we Wrocławiu.
- 3.9. Zmodernizować i uruchomić instalację monitoringu obejmującą Galerię Neonów przy ulicy Ruskiej we Wrocławiu.
- 3.10. Zmodernizować i uruchomić instalację monitoringu obejmującą wnętrze podwórzowe przy ulicy Kazimierza Wielkiego we Wrocławiu (za kinem Nowe Horyzonty).
- 3.11. Rozbudować i uruchomić instalację monitoringu obejmującą teren skateparku przy ulicy Borowskiej we Wrocławiu.
- 3.12. Dostarczyć i uruchomić jeden komplet wyposażenia stanowiska operatorskiego do podglądu obrazu z kamer i współpracy z systemem VMS Genetec Security Center.
- 3.13. Dostarczyć pięć przenośnych stanowisk operatorskich (mobilne stacje robocze) do pracy w systemie VMS Genetec Security Center.
- 3.14. Rozbudować infrastrukturę systemu łączności Monitoringu Prewencyjnego Wrocławia.
- 3.15. Włączyć nowe kamery do systemu VMS Genetec Security Center.

4. Wymagania szczegółowe:

- 4.1. W zakresie budowy i uruchomienia kompleksowej instalacji monitoringu obejmującej Podwórko Wszystkich Mieszkańców zlokalizowane w kwartale ulic Komuny Paryskiej, Miernicza, Łukasińskiego, Prądyńskiego we Wrocławiu należy:
 - 4.1.1. Przeprowadzić procedurę planowania radiowego i wytypować najbardziej korzystną lokalizację do montażu anten systemu łączności radiowej LMDS dla potrzeb transmisji sygnału wideo z kamer monitoringu wizyjnego do systemu centralnego Monitoringu Prewencyjnego Wrocławia.
 - 4.1.2. Zamontować w punkcie kamerowym terminal łączności radiowej LMDS na potrzeby zapewnienia łączności z systemem centralnym. Dostarczone rozwiązanie musi być w pełni kompatybilne z systemem radiowym LMDS posiadanym przez Zamawiającego (rozwiązanie techniczne Intracom Telecom™ typu WiBAS-OSDR). Preferowana lokalizacja urządzeń łączności – budynek przy ul. Mierniczej 18
 - 4.1.3. Zamontować kamerę dwukierunkową na latarni oświetleniowej po zachodniej części boiska
 - 4.1.4. Zamontować kamerę dwukierunkową na latarni oświetleniowej po północnej części boiska
 - 4.1.5. Zamontować kamerę dwukierunkową na latarni oświetleniowej przy budynku ul. Łukasińskiego 9
 - 4.1.6. Zamontować kamerę stałopozycyjną wysokiej rozdzielczości na latarni oświetleniowej przy budynku ul. Łukasińskiego 30f
 - 4.1.7. Zamontować kamerę stałopozycyjną wysokiej rozdzielczości na latarni oświetleniowej przy budynku ul. Miernicza 24
 - 4.1.8. Zastosować system mocowania kamer dedykowany dla danego modelu urządzenia zgodnie z kartami katalogowymi producenta.

- 4.1.9. Obszary obserwacji poszczególnych obiektów kamer ustawiać w porozumieniu i pod nadzorem przedstawiciela Zamawiającego.
- 4.1.10. Wykorzystać istniejącą szafkę teletechniczną zlokalizowaną na terenie podwórza (wydzielona część na potrzeby monitoringu) jako szafkę dostępową.
- 4.1.11. Zamontować wewnątrz szafki dostępowej dedykowane urządzenie aktywne z interfejsem 8xRJ45(10/100M) z HIGH PoE do 90W (zgodne z normą IEEE802.3af, IEEE802.3at, IEEE802.3bt) + 2xSFP (100M/1G/2.5G) o sumarycznej dostępnej mocy na portach PoE nie mniejszej niż 240W, posiadające wbudowane zabezpieczenie przeciwprzepięciowe 4kV 10/700µs ITU K.44 na portach RJ45 w torze transmisyjnym, przystosowane do zasilania redundantnego DC, przystosowane do pracy w warunkach przemysłowych o parametrze MTBF nie mniejszym niż 500 000 godzin, odporne na działanie temperatur w zakresie nie mniejszym niż -25 do +70°C przy zamknięciu w obudowie hermetycznej (brak przepływu powietrza), zapewniające obsługę standardów i protokołów: IEEE 802.1Q VLAN, SNMP v1/v2c/v3.
- 4.1.12. Zamontować wewnątrz szafki dostępowej odpowiednio dobrany zasilacz buforowy na potrzeby zasilania urządzeń w szafce dostępowej o zasilaniu wejściowym jednofazowym 230 V AC, zasilaniu wyjściowym o napięciu nominalnym 48V DC z możliwością regulacji w zakresie nie mniejszym niż 42 do 55V DC, o mocy wyjściowej nie mniejszej niż 500W (pozwalającej na przyszłą rozbudowę instalacji o kolejne urządzenie sieciowe), posiadający sprawność nie mniejszą niż 92%, przystosowany do pracy w zakresie temperatur w zakresie nie mniejszym niż -25 do +70°C, o parametrze MTBF nie mniejszym niż 500 000 godzin, posiadający wbudowane zabezpieczenia: temperaturowe, zwarciove przeciążeniowe, przepięciowe.
- 4.1.13. Wykorzystać istniejące okablowanie do anteny LMDS oraz kamer monitoringu w postaci ekranowanej skrętki miedzianej typu

Ethernet, przystosowanej do układania na zewnątrz, odpornej na warunki atmosferyczne i działanie promieni słonecznych, o parametrach dobranych do zasilanych urządzeń. Okablowanie należy zakończyć wewnątrz szafki dostępowej, zapewniając odpowiedni zapas technologiczny oraz stosując odpowiednio dobrane ochronniki przeciwprzepięciowe dla urządzeń łączności radiowej LMDS.

4.1.14. Zasilanie szafki teletechnicznej w energię elektryczną wykonać z najbliższej zlokalizowanego złącza kablowego. W miejscu przyłączenia do sieci elektrycznej należy wyodrębnić osobny dedykowany obwód zasilania i zamontować podlicznik. Należy zachować zasady stopniowania zabezpieczeń.

4.2. W zakresie budowy i uruchomienia kompleksowej instalacji monitoringu obejmującej wnętrze podwórzowe przy ulicy Kościuszki 35a we Wrocławiu należy:

4.2.1. Przeprowadzić procedurę planowania radiowego i wytypować najbardziej korzystną lokalizację do montażu anten systemu łączności radiowej LMDS dla potrzeb transmisji sygnału wideo z kamer monitoringu wizyjnego do systemu centralnego Monitoringu Prewencyjnego Wrocławia.

4.2.2. Zamontować w punkcie kamerowym terminal łączności radiowej LMDS na potrzeby zapewnienia łączności z systemem centralnym. Dostarczone rozwiązanie musi być w pełni kompatybilne z systemem radiowym LMDS posiadanym przez Zamawiającego (rozwiązanie techniczne Intracom Telecom™ typu WiBAS-OSDR).

4.2.3. Zamontować kamerę wielokierunkową na narożniku budynku przy ul. Kościuszki 35a przy wejściu głównym

4.2.4. Zamontować kamerę stałopozycyjną wysokiej rozdzielczości na elewacji budynku przy ul. Kościuszki 35b/e od strony parkingu za budynkiem (strona zachodnia)

- 4.2.5. Zastosować system mocowania kamer dedykowany dla danego modelu urządzenia zgodnie z kartami katalogowymi producenta.
- 4.2.6. Obszary obserwacji poszczególnych obiektów kamer ustawiać w porozumieniu i pod nadzorem przedstawiciela Zamawiającego.
- 4.2.7. Zamontować w punkcie kamerowym szafkę teletechniczną, która będzie pełnić rolę punktu dostępowego zapewniającego zasilanie kamer oraz transmisję danych do systemu centralnego.
- a) Szafka dostępowa musi być wykonana w całości z metalu, posiadać drzwi zamykane na zamek patentowy, spełniać wymogi ochrony przed warunkami środowiskowymi na poziomie minimum IP54 oraz odporność mechaniczną na poziomie IK10.
 - b) Szafka dostępowa wykonana w I klasie ochronności musi zostać uziemiona zgodnie z wytycznymi producenta.
- 4.2.8. Zamontować wewnątrz szafki dostępowej dedykowane urządzenie aktywne z interfejsem 8xRJ45(10/100M) z HIGH PoE do 90W (zgodne z normą IEEE802.3af, IEEE802.3at, IEEE802.3bt) + 2xSFP (100M/1G/2.5G) o sumarycznej dostępnej mocy na portach PoE nie mniejszej niż 240W, posiadające wbudowane zabezpieczenie przeciwprzepięciowe 4kV 10/700µs ITU K.44 na portach RJ45 w torze transmisyjnym, przystosowane do zasilania redundantnego DC, przystosowane do pracy w warunkach przemysłowych o parametrze MTBF nie mniejszym niż 500 000 godzin, odporne na działanie temperatur w zakresie nie mniejszym niż -25 do +70°C przy zamknięciu w obudowie hermetycznej (brak przepływu powietrza), zapewniające obsługę standardów i protokołów: IEEE 802.1Q VLAN, SNMP v1/v2c/v3.
- 4.2.9. Zamontować wewnątrz szafki dostępowej odpowiednio dobrany zasilacz buforowy na potrzeby zasilania urządzeń w szafce dostępowej o zasilaniu wejściowym jednofazowym 230 V AC, zasilaniu wyjściowym o napięciu nominalnym 48V DC z możliwością regulacji w

zakresie nie mniejszym niż 42 do 55V DC, o mocy wyjściowej nie mniejszej niż 500W (pozwalającej na przyszłą rozbudowę instalacji o kolejne urządzenie sieciowe), posiadający sprawność nie mniejszą niż 92%, przystosowany do pracy w zakresie temperatur w zakresie nie mniejszym niż -25 do +70°C, o parametrze MTBF nie mniejszym niż 500 000 godzin, posiadający wbudowane zabezpieczenia: temperaturowe, zwarciove przeciążeniowe, przepięciowe.

4.2.10. Zastosować okablowanie do anteny LMDS oraz kamer monitoringu w postaci ekranowanej skrętki miedzianej typu Ethernet, przystosowanej do układania na zewnątrz, odpornej na warunki atmosferyczne i działanie promieni słonecznych, o parametrach dobranych do zasilanych urządzeń. Okablowanie należy zakończyć wewnątrz szafki dostępowej, zapewniając odpowiedni zapas technologiczny oraz stosując odpowiednio dobrane ochronniki przeciwprzepięciowe dla urządzeń łączności radiowej LMDS.

4.2.11. Zasilanie szafki teletechnicznej w energię elektryczną wykonać z rozdzielni zasilającej budynek. W miejscu przyłączenia do sieci elektrycznej należy wyodrębnić osobny dedykowany obwód zasilania i zamontować podlicznik. Należy zachować zasady stopniowania zabezpieczeń.

4.3. W zakresie budowy i uruchomienia kompleksowej instalacji monitoringu obejmującej wnętrze podwórzowe przy ulicy Podwale 74 we Wrocławiu należy:

4.3.1. Przeprowadzić procedurę planowania radiowego i wytypować najbardziej korzystną lokalizację do montażu anten systemu łączności radiowej LMDS dla potrzeb transmisji sygnału wideo z kamer monitoringu wizyjnego do systemu centralnego Monitoringu Prewencyjnego Wrocławia.

4.3.2. Zamontować w punkcie kamerowym terminal łączności radiowej LMDS na potrzeby zapewnienia łączności z systemem centralnym. Dostarczone rozwiązanie musi być w pełni kompatybilne

z systemem radiowym LMDS posiadanym przez Zamawiającego (rozwiązanie techniczne Intracom Telecom™ typu WiBAS-OSDR).

- 4.3.3. Zamontować kamerę dwukierunkową na narożniku budynku przy ul. Podwale 74 od strony podwórza (strona północna elewacji budynku)
- 4.3.4. Zamontować kamerę dwukierunkową na narożniku budynku przy ul. Podwale 74 od strony podwórza (strona południowa elewacji budynku)
- 4.3.5. Zastosować system mocowania kamer dedykowany dla danego modelu urządzenia zgodnie z kartami katalogowymi producenta.
- 4.3.6. Obszary obserwacji poszczególnych obiektów kamer należy ustawiać w porozumieniu i pod nadzorem przedstawiciela Zamawiającego.
- 4.3.7. Zamontować w punkcie kamerowym szafkę teletechniczną, która będzie pełnić rolę punktu dostępowego zapewniającego zasilanie kamer oraz transmisję danych do systemu centralnego.
 - a) Szafka dostępową musi być wykonana w całości z metalu, posiadać drzwi zamykane na zamek patentowy, spełniać wymogi ochrony przed warunkami środowiskowymi na poziomie minimum IP54 oraz odporność mechaniczną na poziomie IK10.
 - b) Szafka dostępową wykonaną w I klasie ochronności musi zostać uziemiona zgodnie z wytycznymi producenta.
- 4.3.8. Zamontować wewnątrz szafki dostępowej dedykowane urządzenie aktywne z interfejsem 8xRJ45(10/100M) z HIGH PoE do 90W (zgodne z normą IEEE802.3af, IEEE802.3at, IEEE802.3bt) + 2xSFP (100M/1G/2.5G) o sumarycznej dostępnej mocy na portach PoE nie mniejszej niż 240W, posiadające wbudowane zabezpieczenie przeciwprzepięciowe 4kV 10/700µs ITU K.44 na portach RJ45 w torze transmisyjnym, przystosowane do zasilania redundantnego DC, przystosowane do pracy w warunkach przemysłowych o parametrze

MTBF nie mniejszym niż 500 000 godzin, odporne na działanie temperatur w zakresie nie mniejszym niż -25 do +70°C przy zamknięciu w obudowie hermetycznej (brak przepływu powietrza), zapewniające obsługę standardów i protokołów: IEEE 802.1Q VLAN, SNMP v1/v2c/v3.

4.3.9. Zamontować wewnątrz szafki dostępowej odpowiednio dobrany zasilacz buforowy na potrzeby zasilania urządzeń w szafce dostępowej o zasilaniu wejściowym jednofazowym 230 V AC, zasilaniu wyjściowym o napięciu nominalnym 48V DC z możliwością regulacji w zakresie nie mniejszym niż 42 do 55V DC, o mocy wyjściowej nie mniejszej niż 500W (pozwalającej na przyszłą rozbudowę instalacji o kolejne urządzenie sieciowe), posiadający sprawność nie mniejszą niż 92%, przystosowany do pracy w zakresie temperatur w zakresie nie mniejszym niż -25 do +70°C, o parametrze MTBF nie mniejszym niż 500 000 godzin, posiadający wbudowane zabezpieczenia: temperaturowe, zwarciove przeciążeniowe, przepięciowe.

4.3.10. Zastosować okablowanie do anteny LMDS oraz kamer monitoringu w postaci ekranowanej skrętki miedzianej typu Ethernet, przystosowanej do układania na zewnątrz, odpornej na warunki atmosferyczne i działanie promieni słonecznych, o parametrach dobranych do zasilanych urządzeń. Okablowanie należy zakończyć wewnątrz szafki dostępowej, zapewniając odpowiedni zapas technologiczny oraz stosując odpowiednio dobrane ochronniki przeciwprzepięciowe dla urządzeń łączności radiowej LMDS.

4.3.11. Zasilanie szafki teletechnicznej w energię elektryczną wykonać z rozdzielni zasilającej budynek. W miejscu przyłączenia do sieci elektrycznej należy wyodrębnić osobny dedykowany obwód zasilania i zamontować podlicznik. Należy zachować zasady stopniowania zabezpieczeń.

4.4. W zakresie budowy i uruchomienia kompleksowej instalacji monitoringu obejmującej tereny przyległe do budynku przy ulicy Góralskiej 38 we Wrocławiu należy:

- 4.4.1. Przeprowadzić procedurę planowania radiowego i wytypować najbardziej korzystną lokalizację do montażu anten systemu łączności radiowej LMDS dla potrzeb transmisji sygnału wideo z kamer monitoringu wizyjnego do systemu centralnego Monitoringu Prewencyjnego Wrocławia.
- 4.4.2. Zamontować w punkcie kamerowym terminal łączności radiowej LMDS na potrzeby zapewnienia łączności z systemem centralnym. Dostarczone rozwiązanie musi być w pełni kompatybilne z systemem radiowym LMDS posiadanym przez Zamawiającego (rozwiązanie techniczne Intracom Telecom™ typu WiBAS-OSDR).
- 4.4.3. Zamontować w punkcie kamerowym kamerę wielokierunkową na narożniku budynku przy ul. Góralskiej 38 od strony ulicy.
- 4.4.4. Zastosować system mocowania kamer dedykowany dla danego modelu urządzenia zgodnie z kartami katalogowymi producenta.
- 4.4.5. Obszary obserwacji poszczególnych obiektów kamer należy ustawiać w porozumieniu i pod nadzorem przedstawiciela Zamawiającego.
- 4.4.6. Zamontować w punkcie kamerowym szafkę teletechniczną, która będzie pełnić rolę punktu dostępowego zapewniającego zasilanie kamer oraz transmisję danych do systemu centralnego.
- a) Szafka dostępową musi być wykonana w całości z metalu, posiadać drzwi zamykane na zamek patentowy, spełniać wymogi ochrony przed warunkami środowiskowymi na poziomie minimum IP54 oraz odporność mechaniczną na poziomie IK10.
 - b) Szafka dostępową wykonaną w I klasie ochronności musi zostać uziemiona zgodnie z wytycznymi producenta.
- 4.4.7. Zamontować wewnątrz szafki dostępowej dedykowane urządzenie aktywne z interfejsem 8xRJ45(10/100M) z HIGH PoE do 90W (zgodne z normą IEEE802.3af, IEEE802.3at, IEEE802.3bt) + 2xSFP (100M/1G/2.5G) o sumarycznej dostępnej mocy na portach

PoE nie mniejszej niż 240W, posiadające wbudowane zabezpieczenie przeciwprzepięciowe 4kV 10/700µs ITU K.44 na portach RJ45 w torze transmisyjnym, przystosowane do zasilania redundantnego DC, przystosowane do pracy w warunkach przemysłowych o parametrze MTBF nie mniejszym niż 500 000 godzin, odporne na działanie temperatur w zakresie nie mniejszym niż -25 do +70°C przy zamknięciu w obudowie hermetycznej (brak przepływu powietrza), zapewniające obsługę standardów i protokołów: IEEE 802.1Q VLAN, SNMP v1/v2c/v3.

- 4.4.8. Zamontować wewnątrz szafki dostępowej odpowiednio dobrany zasilacz buforowy na potrzeby zasilania urządzeń w szafce dostępowej o zasilaniu wejściowym jednofazowym 230 V AC, zasilaniu wyjściowym o napięciu nominalnym 48V DC z możliwością regulacji w zakresie nie mniejszym niż 42 do 55V DC, o mocy wyjściowej nie mniejszej niż 500W (pozwalającej na przyszłą rozbudowę instalacji o kolejne urządzenie sieciowe), posiadający sprawność nie mniejszą niż 92%, przystosowany do pracy w zakresie temperatur w zakresie nie mniejszym niż -25 do +70°C, o parametrze MTBF nie mniejszym niż 500 000 godzin, posiadający wbudowane zabezpieczenia: temperaturowe, zwarciove przeciążeniowe, przepięciowe.
- 4.4.9. Zastosować okablowanie do anteny LMDS oraz kamer monitoringu w postaci ekranowanej skrętki miedzianej typu Ethernet, przystosowanej do układania na zewnątrz, odpornej na warunki atmosferyczne i działanie promieni słonecznych, o parametrach dobranych do zasilanych urządzeń. Okablowanie należy zakończyć wewnątrz szafki dostępowej, zapewniając odpowiedni zapas technologiczny oraz stosując odpowiednio dobrane ochronniki przeciwprzepięciowe dla urządzeń łączności radiowej LMDS.
- 4.4.10. Zasilanie szafki teletechnicznej w energię elektryczną wykonać z rozdzielni zasilającej budynek. W miejscu przyłączenia do sieci elektrycznej należy wyodrębnić osobny dedykowany obwód zasilania i zamontować podlicznik. Należy zachować zasady stopniowania zabezpieczeń.

4.5. W zakresie budowy i uruchomienia kompleksowej instalacji monitoringu obejmującej skrzyżowanie ulicy Kolejowej z placem Rozjezdnym we Wrocławiu należy:

4.5.1. Przeprowadzić procedurę planowania radiowego i wytypować najbardziej korzystną lokalizację do montażu anten systemu łączności radiowej LMDS dla potrzeb transmisji sygnału wideo z kamer monitoringu wizyjnego do systemu centralnego Monitoringu Prewencyjnego Wrocławia.

4.5.2. Zamontować w punkcie kamerowym terminal łączności radiowej LMDS na potrzeby zapewnienia łączności z systemem centralnym. Dostarczone rozwiązanie musi być w pełni kompatybilne z systemem radiowym LMDS posiadanym przez Zamawiającego (rozwiązanie techniczne Intracom Telecom™ typu WiBAS-OSDR).

4.5.3. Zamontować w punkcie kamerowym kamerę wielokierunkową. Preferowana lokalizacja – słup oświetleniowy 302/120.

4.5.4. Zastosować system mocowania kamer dedykowany dla danego modelu urządzenia zgodnie z kartami katalogowymi producenta.

4.5.5. Obszary obserwacji poszczególnych obiektów kamer ustawiać w porozumieniu i pod nadzorem przedstawiciela Zamawiającego.

4.5.6. Zamontować w punkcie kamerowym szafkę teletechniczną, która będzie pełnić rolę punktu dostępowego zapewniającego zasilanie kamer oraz transmisję danych do systemu centralnego.

- a) Szafka dostępową musi być wykonana w całości z metalu, posiadać drzwi zamykane na zamek patentowy, spełniać wymogi ochrony przed warunkami środowiskowymi na poziomie minimum IP54 oraz odporność mechaniczną na poziomie IK10.
- b) Szafka dostępową wykonaną w I klasie ochronności musi zostać uziemiona zgodnie z wytycznymi producenta.

- 4.5.7. Zamontować wewnątrz szafki dostępowej dedykowane urządzenie aktywne z interfejsem 8xRJ45(10/100M) z HIGH PoE do 90W (zgodne z normą IEEE802.3af, IEEE802.3at, IEEE802.3bt) + 2xSFP (100M/1G/2.5G) o sumarycznej dostępnej mocy na portach PoE nie mniejszej niż 240W, posiadające wbudowane zabezpieczenie przeciwprzepięciowe 4kV 10/700µs ITU K.44 na portach RJ45 w torze transmisyjnym, przystosowane do zasilania redundantnego DC, przystosowane do pracy w warunkach przemysłowych o parametrze MTBF nie mniejszym niż 500 000 godzin, odporne na działanie temperatur w zakresie nie mniejszym niż -25 do +70°C przy zamknięciu w obudowie hermetycznej (brak przepływu powietrza), zapewniające obsługę standardów i protokołów: IEEE 802.1Q VLAN, SNMP v1/v2c/v3.
- 4.5.8. Zamontować wewnątrz szafki dostępowej odpowiednio dobrany zasilacz buforowy na potrzeby zasilania urządzeń w szafce dostępowej o zasilaniu wejściowym jednofazowym 230 V AC, zasilaniu wyjściowym o napięciu nominalnym 48V DC z możliwością regulacji w zakresie nie mniejszym niż 42 do 55V DC, o mocy wyjściowej nie mniejszej niż 500W (pozwalającej na przyszłą rozbudowę instalacji o kolejne urządzenie sieciowe), posiadający sprawność nie mniejszą niż 92%, przystosowany do pracy w zakresie temperatur w zakresie nie mniejszym niż -25 do +70°C, o parametrze MTBF nie mniejszym niż 500 000 godzin, posiadający wbudowane zabezpieczenia: temperaturowe, zwarciove przeciążeniowe, przepięciowe.
- 4.5.9. W szafce dostępowej należy umieścić zestaw akumulatorów typu LiFePO pozwalający na podtrzymanie zasilania przez nie mniej niż 24 godziny przy maksymalnym poziomie naładowania akumulatorów.
- 4.5.10. Zastosować okablowanie do anteny LMDS oraz kamer monitoringu w postaci ekranowanej skrętki miedzianej typu Ethernet, przystosowanej do układania na zewnątrz, odpornej na warunki atmosferyczne i działanie promieni słonecznych, o parametrach dobranych do zasilanych urządzeń. Okablowanie należy zakończyć

wewnątrz szafki dostępowej, zapewniając odpowiedni zapas technologiczny oraz stosując odpowiednio dobrane ochronniki przeciwprzepięciowe dla urządzeń łączności radiowej LMDS.

4.5.11. Zasilanie szafki teletechnicznej w energię elektryczną wykonać z obwodu oświetlenia ulicznego. Należy zachować zasady stopniowania zabezpieczeń.

4.6. W zakresie budowy i uruchomienia kompleksowej instalacji monitoringu obejmującej skrzyżowanie ulicy Bystrzyckiej i Metalowców we Wrocławiu należy:

4.6.1. Przeprowadzić procedurę planowania radiowego i wytypować najbardziej korzystną lokalizację do montażu anten systemu łączności radiowej LMDS dla potrzeb transmisji sygnału wideo z kamer monitoringu wizyjnego do systemu centralnego Monitoringu Prewencyjnego Wrocławia.

4.6.2. Rozbudować stację bazową LMDS przy ul. Muchoborskiej o dodatkowy sektor dedykowany do obsługi nowego punktu kamerowego. Dostarczone rozwiązanie musi być w pełni kompatybilne z systemem radiowym LMDS posiadanym przez Zamawiającego (rozwiązanie techniczne Intracom Telecom™ typu WiBAS-OSDR).

4.6.3. Zamontować w punkcie kamerowym terminal łączności radiowej LMDS na potrzeby zapewnienia łączności z systemem centralnym. Dostarczone rozwiązanie musi być w pełni kompatybilne z systemem radiowym LMDS posiadanym przez Zamawiającego (rozwiązanie techniczne Intracom Telecom™ typu WiBAS-OSDR).

4.6.4. Zamontować kamerę wielokierunkową. Preferowana lokalizacja – słup oświetleniowy 229/106.

4.6.5. Zastosować system mocowania kamer dedykowany dla danego modelu urządzenia zgodnie z kartami katalogowymi producenta.

- 4.6.6. Obszary obserwacji poszczególnych obiektów kamer ustawiać w porozumieniu i pod nadzorem przedstawiciela Zamawiającego.
- 4.6.7. Zamontować w punkcie kamerowym szafkę teletechniczną, która będzie pełnić rolę punktu dostępowego zapewniającego zasilanie kamer oraz transmisję danych do systemu centralnego.
- a) Szafka dostępową musi być wykonana w całości z metalu, posiadać drzwi zamykane na zamek patentowy, spełniać wymogi ochrony przed warunkami środowiskowymi na poziomie minimum IP54 oraz odporność mechaniczną na poziomie IK10.
 - b) Szafka dostępową wykonaną w I klasie ochronności musi zostać uziemiona zgodnie z wytycznymi producenta.
- 4.6.8. Zamontować wewnątrz szafki dostępowej dedykowane urządzenie aktywne z interfejsem 8xRJ45(10/100M) z HIGH PoE do 90W (zgodne z normą IEEE802.3af, IEEE802.3at, IEEE802.3bt) + 2xSFP (100M/1G/2.5G) o sumarycznej dostępnej mocy na portach PoE nie mniejszej niż 240W, posiadające wbudowane zabezpieczenie przeciwprzepięciowe 4kV 10/700µs ITU K.44 na portach RJ45 w torze transmisyjnym, przystosowane do zasilania redundantnego DC, przystosowane do pracy w warunkach przemysłowych o parametrze MTBF nie mniejszym niż 500 000 godzin, odporne na działanie temperatur w zakresie nie mniejszym niż -25 do +70°C przy zamknięciu w obudowie hermetycznej (brak przepływu powietrza), zapewniające obsługę standardów i protokołów: IEEE 802.1Q VLAN, SNMP v1/v2c/v3.
- 4.6.9. Zamontować wewnątrz szafki dostępowej odpowiednio dobrany zasilacz buforowy na potrzeby zasilania urządzeń w szafce dostępowej o zasilaniu wejściowym jednofazowym 230 V AC, zasilaniu wyjściowym o napięciu nominalnym 48V DC z możliwością regulacji w zakresie nie mniejszym niż 42 do 55V DC, o mocy wyjściowej nie mniejszej niż 500W (pozwalającej na przyszłą rozbudowę instalacji o kolejne urządzenie sieciowe), posiadający sprawność nie mniejszą niż

92%, przystosowany do pracy w zakresie temperatur w zakresie nie mniejszym niż -25 do +70°C, o parametrze MTBF nie mniejszym niż 500 000 godzin, posiadający wbudowane zabezpieczenia: temperaturowe, zwarciove przeciążeniowe, przepięciowe.

4.6.10. W szafce dostępowej należy umieścić zestaw akumulatorów typu LiFePO pozwalający na podtrzymanie zasilania przez nie mniej niż 24 godziny przy maksymalnym poziomie naładowania akumulatorów.

4.6.11. Zastosować okablowanie do anteny LMDS oraz kamer monitoringu w postaci ekranowanej skrętki miedzianej typu Ethernet, przystosowanej do układania na zewnątrz, odpornej na warunki atmosferyczne i działanie promieni słonecznych, o parametrach dobranych do zasilanych urządzeń. Okablowanie należy zakończyć wewnątrz szafki dostępowej, zapewniając odpowiedni zapas technologiczny oraz stosując odpowiednio dobrane ochronniki przeciwprzepięciowe dla urządzeń łączności radiowej LMDS.

4.6.12. Zasilanie szafki teletechnicznej w energię elektryczną wykonać z obwodu oświetlenia ulicznego. Należy zachować zasady stopniowania zabezpieczeń.

4.7. W zakresie budowy i uruchomienia kompleksowej instalacji monitoringu obejmującej tereny przyległe do Jazu Małgorzata we Wrocławiu należy:

4.7.1. Przeprowadzić procedurę planowania radiowego i wytypować najbardziej korzystną lokalizację do montażu anten systemu łączności radiowej LMDS dla potrzeb transmisji sygnału wideo z kamer monitoringu wizyjnego do systemu centralnego Monitoringu Prewencyjnego Wrocławia.

4.7.2. Zamontować w punkcie kamerowym kamerę wielokierunkową na narożniku budynku technicznego (od strony budowli hydrotechnicznej).

- 4.7.3. Zamontować w punkcie kamerowym kamerę wielokierunkową na narożniku budynku technicznego (od strony lądowiska dla śmigłowców ratowniczych).
- 4.7.4. Zamontować w punkcie kamerowym kamerę PTZ na narożniku budynku technicznego (od strony rzeki).
- 4.7.5. Zastosować system mocowania kamer dedykowany dla danego modelu urządzenia zgodnie z kartami katalogowymi producenta.
- 4.7.6. Przy każdej z kamer wielokierunkowych zamontować zewnętrzny głośnik sieciowy.
- 4.7.7. Obszary obserwacji poszczególnych obiektów kamer należy ustawiać w porozumieniu i pod nadzorem przedstawiciela Zamawiającego.
- 4.7.8. Zamontować w punkcie kamerowym szafkę teletechniczną, która będzie pełnić rolę punktu dostępowego zapewniającego zasilanie kamer oraz transmisję danych do systemu centralnego.
- a) Szafka dostępową musi być wykonana w całości z metalu, posiadać drzwi zamykane na zamek patentowy, spełniać wymogi ochrony przed warunkami środowiskowymi na poziomie minimum IP54 oraz odporność mechaniczną na poziomie IK10.
 - b) Szafka dostępową wykonaną w I klasie ochronności musi zostać uziemiona zgodnie z wytycznymi producenta.
- 4.7.9. Zamontować wewnątrz szafki dostępowej dedykowane urządzenie aktywne z interfejsem 8xRJ45(10/100M) z HIGH PoE do 90W (zgodne z normą IEEE802.3af, IEEE802.3at, IEEE802.3bt) + 2xSFP (100M/1G/2.5G) o sumarycznej dostępnej mocy na portach PoE nie mniejszej niż 240W, posiadające wbudowane zabezpieczenie przeciwprzepięciowe 4kV 10/700µs ITU K.44 na portach RJ45 w torze transmisyjnym, przystosowane do zasilania redundantnego DC, przystosowane do pracy w warunkach przemysłowych o parametrze MTBF nie mniejszym niż 500 000 godzin, odporne na działanie

temperatur w zakresie nie mniejszym niż -25 do +70°C przy zamknięciu w obudowie hermetycznej (brak przepływu powietrza), zapewniające obsługę standardów i protokołów: IEEE 802.1Q VLAN, SNMP v1/v2c/v3.

- 4.7.10. Zamontować wewnątrz szafki dostępowej odpowiednio dobrany zasilacz buforowy na potrzeby zasilania urządzeń w szafce dostępowej o zasilaniu wejściowym jednofazowym 230 V AC, zasilaniu wyjściowym o napięciu nominalnym 48V DC z możliwością regulacji w zakresie nie mniejszym niż 42 do 55V DC, o mocy wyjściowej nie mniejszej niż 500W (pozwalającej na przyszłą rozbudowę instalacji o kolejne urządzenie sieciowe), posiadający sprawność nie mniejszą niż 92%, przystosowany do pracy w zakresie temperatur w zakresie nie mniejszym niż -25 do +70°C, o parametrze MTBF nie mniejszym niż 500 000 godzin, posiadający wbudowane zabezpieczenia: temperaturowe, zwarciove przeciążeniowe, przepięciowe.
- 4.7.11. Zastosować okablowanie do anteny LMDS oraz kamer monitoringu w postaci ekranowanej skrętki miedzianej typu Ethernet, przystosowanej do układania na zewnątrz, odpornej na warunki atmosferyczne i działanie promieni słonecznych, o parametrach dobranych do zasilanych urządzeń. Okablowanie należy zakończyć wewnątrz szafki dostępowej, zapewniając odpowiedni zapas technologiczny oraz stosując odpowiednio dobrane ochronniki przeciwprzepięciowe dla urządzeń łączności radiowej LMDS.
- 4.7.12. Zasilanie szafki teletechnicznej w energię elektryczną wykonać z rozdzielni zasilającej budynek. W miejscu przyłączenia do sieci elektrycznej należy wyodrębnić osobny dedykowany obwód zasilania i zamontować podlicznik. Należy zachować zasady stopniowania zabezpieczeń.
- 4.7.13. Łączność z systemem centralnym należy wykonać za pomocą pary urządzeń PtP typu StreetNode pracujących w licencjonowanym paśmie LMDS 28 GHz w relacji Jaz Małgorzata – Komisariat Policji Wrocław Rakowiec (punkt retransmisyjny).

4.7.14. Zamontować w punkcie retransmisyjnym szafkę teletechniczną, która będzie pełnić rolę punktu dostępowego zapewniającego zasilanie urządzenia łączności typu StreetNode oraz transmisję danych do systemu centralnego.

- a) Szafka teletechniczna musi być wykonana w całości z metalu, posiadać drzwi zamykane na zamek patentowy, spełniać wymogi ochrony przed warunkami środowiskowymi na poziomie minimum IP54 oraz odporność mechaniczną na poziomie IK10.
- b) Szafka teletechniczna wykonana w I klasie ochronności musi zostać uziemiona zgodnie z wytycznymi producenta.

4.7.15. Zamontować wewnątrz szafki teletechnicznej dedykowane urządzenie aktywne z interfejsem 8xRJ45(10/100M) z HIGH PoE do 90W (zgodne z normą IEEE802.3af, IEEE802.3at, IEEE802.3bt) + 2xSFP (100M/1G/2.5G) o sumarycznej dostępnej mocy na portach PoE nie mniejszej niż 240W, posiadające wbudowane zabezpieczenie przeciwprzepięciowe 4kV 10/700µs ITU K.44 na portach RJ45 w torze transmisyjnym, przystosowane do zasilania redundantnego DC, przystosowane do pracy w warunkach przemysłowych o parametrze MTBF nie mniejszym niż 500 000 godzin, odporne na działanie temperatur w zakresie nie mniejszym niż -25 do +70°C przy zamknięciu w obudowie hermetycznej (brak przepływu powietrza), zapewniające obsługę standardów i protokołów: IEEE 802.1Q VLAN, SNMP v1/v2c/v3.

4.7.16. Zamontować wewnątrz szafki teletechnicznej odpowiednio dobrany zasilacz buforowy na potrzeby zasilania urządzeń w szafce dostępowej o zasilaniu wejściowym jednofazowym 230 V AC, zasilaniu wyjściowym o napięciu nominalnym 48V DC z możliwością regulacji w zakresie nie mniejszym niż 42 do 55V DC, o mocy wyjściowej nie mniejszej niż 500W (pozwalającej na przyszłą rozbudowę instalacji o kolejne urządzenie sieciowe), posiadający sprawność nie mniejszą niż 92%, przystosowany do pracy w zakresie temperatur w zakresie nie mniejszym niż -25 do +70°C, o parametrze MTBF nie mniejszym niż

500 000 godzin, posiadający wbudowane zabezpieczenia:
temperaturowe, zwarciove przeciążeniowe, przepięciowe.

4.7.17. Komunikację z systemem centralnym należy zaprojektować i wykonać z szafki teletechnicznej jako dedykowane łącze światłowodowe.

4.8. W zakresie budowy i uruchomienia łącza radiowego LMDS na potrzeby punktu kamerowego przy ulicy Wielkopolskiej 16 we Wrocławiu należy:

4.8.1. Połączenie należy wykonać za pomocą pary urządzeń PtP typu StreetNode pracujących w licencjonowanym paśmie LMDS 28 GHz w relacji Kosmonautów 274 – Wielkopolska 16.

4.8.2. Po stronie obiektu przy ul. Kosmonautów 274 należy zamontować szafkę dostępową wraz z wyposażeniem oraz antenę StreetNode LMDS.

4.8.3. Antenę StreetNode LMDS należy umieścić na maszcie radiowym na dachu budynku.

4.8.4. Szafkę dostępową należy umieścić w wyznaczonym pomieszczeniu technicznym.

4.8.5. Szafka dostępowa musi być wykonana w całości z metalu, posiadać drzwi zamykane na zamek patentowy, spełniać wymogi ochrony przed warunkami środowiskowymi na poziomie minimum IP54 oraz odporność mechaniczną na poziomie IK10. Szafka dostępowa wykonana w I klasie ochronności musi zostać uziemiona zgodnie z wytycznymi producenta.

4.8.6. Wewnątrz szafki dostępowej należy umieścić dedykowane urządzenie aktywne z interfejsem 8xRJ45(10/100M) z HIGH PoE do 90W (zgodne z normą IEEE802.3af, IEEE802.3at, IEEE802.3bt) + 2xSFP (100M/1G/2.5G) o sumarycznej dostępnej mocy na portach PoE nie mniejszej niż 240W, posiadające wbudowane zabezpieczenie przeciwprzepięciowe 4kV 10/700µs ITU K.44 na portach RJ45 w torze transmisyjnym, przystosowane do zasilania redundantnego DC, przystosowane do pracy w warunkach przemysłowych o parametrze

MTBF nie mniejszym niż 500 000 godzin, odporne na działanie temperatur w zakresie nie mniejszym niż -25 do +70°C przy zamknięciu w obudowie hermetycznej (brak przepływu powietrza), zapewniające obsługę standardów i protokołów: IEEE 802.1Q VLAN, SNMP v1/v2c/v3.

- 4.8.7. Wewnątrz szafki dostępowej należy zamontować odpowiednio dobrany zasilacz na potrzeby zasilania urządzeń w szafce dostępowej o zasilaniu wejściowym jednofazowym 230 V AC, zasilaniu wyjściowym o napięciu nominalnym 48V DC z możliwością regulacji w zakresie nie mniejszym niż 42 do 55V DC, o mocy wyjściowej nie mniejszej niż 500W (pozwalającej na przyszłą rozbudowę instalacji o kolejne urządzenie sieciowe), posiadający sprawność nie mniejszą niż 92%, przystosowany do pracy w zakresie temperatur w zakresie nie mniejszym niż -25 do +70°C, o parametrze MTBF nie mniejszym niż 500 000 godzin, posiadający wbudowane zabezpieczenia: temperaturowe, zwarciove przeciążeniowe, przepięciowe.
- 4.8.8. Zasilanie szafki dostępowej w energię elektryczną należy wykonać z najbliższego dostępnego złącza elektrycznego / rozdzielni. W miejscu przyłączenia do sieci elektrycznej należy wpiąć instalację w dedykowany obwód zasilania. Należy zachować zasady stopniowania zabezpieczeń.
- 4.8.9. Komunikację z systemem centralnym należy zaprojektować i wykonać z jednej z szafek dostępowych jako dedykowane łącze światłowodowe.
- 4.8.10. Po stronie obiektu przy ul. Wielkopolskiej 16 należy zamontować antenę StreetNode.
- 4.8.11. Urządzenie należy wpiąć do lokalnej instalacji teletechnicznej realizowanej na potrzeby projektu WBO obejmującego budowę księżkomatu wraz z instalacją monitoringu wizyjnego w obrębie strefy wejściowej do Parku Literatów. Wymagana koordynacja z zadaniem realizowanym przez innego wykonawcę na rzecz Gminy Wrocław reprezentowanej przez Zamawiającego.

4.9. W zakresie modernizacji i uruchomienia instalacji monitoringu obejmującej Galerię Neonów przy ulicy Ruskiej we Wrocławiu:

4.9.1. Przed rozpoczęciem prac Wykonawca zobowiązany jest dokonać sprawdzenia istniejących elementów infrastruktury technicznej wchodzącej w skład istniejącej instalacji monitoringu wizyjnego (w szczególności szafki teletechniczne, okablowanie transmisyjne, obwody zasilania)

4.9.2. Wszelkie wyeksploatowane, uszkodzone lub nienadające się do wykorzystania elementy infrastruktury należy wymienić na nowe.

4.9.3. Należy zmodernizować dwie szafki dostępne zlokalizowane w budynkach przy ul. Ruskiej 46a oraz Ruskiej 46c.

4.9.4. Wewnątrz szafek dostępowych należy umieścić po jednym dedykowanym urządzeniu aktywnym z interfejsem 8xRJ45(10/100M) z HIGH PoE do 90W (zgodne z normą IEEE802.3af, IEEE802.3at, IEEE802.3bt) + 2xSFP (100M/1G/2.5G) o sumarycznej dostępnej mocy na portach PoE nie mniejszej niż 240W, posiadające wbudowane zabezpieczenie przeciwprzepięciowe 4kV 10/700µs ITU K.44 na portach RJ45 w torze transmisyjnym, przystosowane do zasilania redundantnego DC, przystosowane do pracy w warunkach przemysłowych o parametrze MTBF nie mniejszym niż 500 000 godzin, odporne na działanie temperatur w zakresie nie mniejszym niż -25 do +70°C przy zamknięciu w obudowie hermetycznej (brak przepływu powietrza), zapewniające obsługę standardów i protokołów: IEEE 802.1Q VLAN, SNMP v1/v2c/v3.

4.9.5. Wewnątrz szafek dostępowych należy zamontować po jednym odpowiednio dobranym zasilaczu na potrzeby zasilania urządzeń w szafce dostępowej o zasilaniu wejściowym jednofazowym 230 V AC, zasilaniu wyjściowym o napięciu nominalnym 48V DC z możliwością regulacji w zakresie nie mniejszym niż 42 do 55V DC, o mocy wyjściowej nie mniejszej niż 500W (pozwalającej na przyszłą rozbudowę instalacji o kolejne urządzenie sieciowe), posiadający sprawność nie mniejszą niż 92%, przystosowany do pracy w zakresie

temperatur w zakresie nie mniejszym niż -25 do +70°C, o parametrze MTBF nie mniejszym niż 500 000 godzin, posiadający wbudowane zabezpieczenia: temperaturowe, zwarciove przeciążeniowe, przepięciowe.

- 4.9.6. Istniejące szafki dostępne należy wymienić na nowe w przypadku braku odpowiedniej ilości miejsca na montaż w/w urządzeń lub braku spełniania minimalnych wymagań technicznych dla szafek dostępowych.
- 4.9.7. Szafki dostępne muszą być wykonane w całości z metalu, posiadać drzwi zamykane na zamek patentowy, spełniać wymogi ochrony przed warunkami środowiskowymi na poziomie minimum IP54 oraz odporność mechaniczną na poziomie IK10. Szafki dostępne wykonane w I klasie ochronności muszą zostać uziemione zgodnie z wytycznymi producenta.
- 4.9.8. Komunikację z systemem centralnym należy zaprojektować i wykonać z jednej z szafek dostępowych jako dedykowane łącze światłowodowe.
- 4.9.9. W przypadku braku możliwości technicznych wykonania przyłącza światłowodowego, komunikację z systemem centralnym należy zrealizować jako łącze radiowe pracujące w systemie łączności radiowej LMDS Zamawiającego. Antenę radiolinii LMDS należy zlokalizować na dachu budynku przy ul. Ruskiej 46a lub Ruskiej 46c i podłączyć odpowiednio do właściwego punktu dostępowego.
- 4.9.10. Należy stosować okablowanie do anten LMDS oraz kamer monitoringu w postaci ekranowanej skrętki miedzianej typu Ethernet, przystosowanej do układania na zewnątrz, odpornej na warunki atmosferyczne i działanie promieni słonecznych, o parametrach dobranych do zasilanych urządzeń. Okablowanie należy zakończyć wewnątrz szafki dostępowej, zapewniając odpowiedni zapas technologiczny oraz stosując odpowiednio dobrane ochronniki przeciwprzepięciowe dla urządzeń łączności radiowej LMDS.

- 4.9.11. Kamery stałopozycyjne K1, K2, K3 i K7 należy wymienić na nowe kamery stałopozycyjne o wysokiej rozdzielczości.
- 4.9.12. Kamery stałopozycyjne K4, K5 oraz K6 należy zastąpić jedną kamerą wielokierunkową.
- 4.9.13. Należy zamontować dodatkową kamerę stałopozycyjną wysokiej rozdzielczości na narożniku budynku przy ul. Ruskiej 47 obejmującą polem widzenia część podwórza po stronie wschodniej w sąsiedztwie lokali gastronomicznych.
- 4.9.14. Połączenie kablowe do nowej kamery należy wykonać z szafki dostępowej zlokalizowanej w budynku przy ul. Ruskiej 46a lub Ruskiej 46c. W przypadku realizacji połączenia z szafki dostępowej przy ul. Ruskiej 46a należy wykonać to połączenie w postaci przewieszki między budynkami.
- 4.10. W zakresie modernizacji i uruchomienia instalacji monitoringu obejmującej wnętrze podwórzowe przy ulicy Kazimierza Wielkiego we Wrocławiu (za kinem Nowe Horyzonty):
 - 4.10.1. Przed rozpoczęciem prac należy dokonać sprawdzenia istniejących elementów infrastruktury technicznej wchodzącej w skład istniejącej instalacji monitoringu wizyjnego (w szczególności szafki teletechniczne, okablowanie transmisyjne, obwody zasilania)
 - 4.10.2. Wszelkie wyeksploatowane, uszkodzone lub nienadające się do wykorzystania elementy infrastruktury należy wymienić na nowe.
 - 4.10.3. Istniejącą kamerę PTZ (kamera 1-0026) Monitoringu Prewencyjnego Wrocławia należy wymienić na nową kamerę wielokierunkową.
 - 4.10.4. Obszary obserwacji poszczególnych obiektów kamer należy ustawiać w porozumieniu i pod nadzorem przedstawiciela Zamawiającego.
 - 4.10.5. Nową kamerę należy podłączyć do istniejącej instalacji Monitoringu Prewencyjnego Wrocławia znajdującej się w tej lokalizacji.

- 4.10.6. Należy dokonać rekonfiguracji istniejącego systemu łączności radiowej LMDS w celu zapewnienia odpowiednich parametrów pracy urządzeń i przepustowości łącza radiowego.
- 4.11. W zakresie rozbudowy i uruchomienia instalacji monitoringu obejmującej teren skateparku przy ulicy Borowskiej we Wrocławiu:
- 4.11.1. Dodatkową kamerę PTZ należy zamontować na górze słupa oświetleniowego, na którym znajduje się istniejąca szafka teletechniczna Monitoringu Prewencyjnego Wrocławia.
- 4.11.2. Miejsce montażu kamer należy dobrać w taki sposób, aby pole widzenia kamery w maksymalnym stopniu umożliwiała obserwację terenu placówki oświatowej sąsiadującej ze skateparkiem.
- 4.11.3. Nową kamerę należy podłączyć do istniejącej instalacji Monitoringu Prewencyjnego Wrocławia znajdującej się w tej lokalizacji.
- 4.11.4. Należy dokonać rekonfiguracji istniejącego systemu łączności radiowej LMDS w celu zapewnienia odpowiednich parametrów pracy urządzeń i przepustowości łącza radiowego.
- 4.12. W zakresie dostawy i uruchomienia jednego kompletnego wyposażenia stanowiska operatorskiego do podglądu obrazu z kamer i współpracy z systemem VMS Genetec Security Center należy:
- 4.12.1. Dostarczyć jedną stację roboczą o minimalnych parametrach użytkowych: CPU i7-14 gen., RAM 16GB DDR5, HDD 512GB SSD, GPU RTX A1000 8GB, OS Windows 11 Pro, DVD R/W, monitor 27" UHD.
- 4.12.2. Zainstalować niezbędne oprogramowanie oraz skonfigurować stację roboczą do pracy z systemem Genetec Security Center Zamawiającego.
- 4.12.3. Zamontować i uruchomić urządzenie we wskazanej lokalizacji na terenie Komisariatu Policji Wrocław Rakowiec.

- 4.12.4. Stację roboczą podłączyć sieciowo do szafki teletechnicznej wybudowanej w ramach realizacji punktu retransmisyjnego dla instalacji monitoringu obejmującej Jaz Małgorzata.
- 4.13. W zakresie dostawy pięciu przenośnych stanowisk operatorskich (mobilne stacje robocze) do pracy w systemie VMS Genetec Security Center należy:
- 4.13.1. Dostarczyć pięć mobilnych stacji roboczych o minimalnych parametrach użytkowych: CPU Ultra 7-266V , RAM 16GB DDR5, HDD 512GB SSD M.2, GPU Arc, karta WLAN 802.11be, Bluetooth 5.4, wbudowany czytnik linii papilarnych oraz smart card, wbudowany touch pad, podświetlana klawiatura, wbudowana kamera 1080p, wbudowana bateria o pojemności 55Wh, wbudowane złącza 2xUSB-C + 2xUSB-A + 1xHDMI, OS Windows 11 Pro, wbudowany ekran dotykowy z powłoką anti-glare o przekątnej nie większej niż 14" i minimalnej rozdzielczości FullHD+, wytrzymała obudowa o konstrukcji wykonanej z aluminium, waga nie większa niż 1,5 kg.
- 4.13.2. Do każdej mobilnej stacji roboczej dostarczyć myszkę optyczną o rozdzielczości 4000 DPI z bezprzewodowymi interfejsami bluetooth oraz wireless pochodzącą z linii produktowej producenta mobilnej stacji roboczej.
- 4.13.3. Do każdej mobilnej stacji roboczej adapter z portami rozszerzeń: 1x HDMI + 1x DisplayPort + 1x VGA + 1x LAN RJ-45 1GB/s + 1x USB-C + 1x USB-A pochodzący z linii produktowej producenta mobilnej stacji roboczej.
- 4.13.4. Do każdej mobilnej stacji roboczej dostarczyć dedykowaną torbę z uchwytem na ramię do przenoszenia urządzenia pochodzącą z linii produktowej producenta mobilnej stacji roboczej.
- 4.14. W zakresie niezbędnej rozbudowy infrastruktury systemu łączności Monitoringu Prewencyjnego Wrocławia należy:

4.14.1. Dostarczyć dwa 24-portowe przełączniki sieciowe pozwalające na rozbudowę systemu łączności Monitoringu Prewencyjnego Wrocławia.

4.14.2. Minimalne wymagane parametry techniczne dla 24-portowych przełączników sieciowych:

- a) wysokość urządzenia 1U (rack 19")
- b) Przełącznik wyposażony w:
 - minimum 24 interfejsy 10/100/1000Base-T RJ45 PoE+
 - minimum 8 interfejsów 10GB Base-X SFP+
- c) możliwość łączenia do 8 urządzeń w stos zarządzany z pojedynczego adresu IP, połączenie pomiędzy poszczególnymi urządzeniami musi być możliwe z przepustowością minimum 40Gbps
- d) nieblokująca architektura o wydajności przełączania min. 208 Gbps i matrycy przełączającej z szybkością minimum 154 milionów pakietów na sekundę (Mpps)
- e) pojemność tablicy ARP: minimum 8000 wpisów
- f) pojemność tablicy adresów MAC: minimum 32 000 wpisów
- g) możliwość przypisania minimum 1000 ACL (sumarycznie wejściowe i wyjściowe)
- h) minimum 8000 wpisów w tablicy routingu IPv4
- i) minimum 4000 wpisów w tablicy routingu IPv6
- j) obsługa routingu IPv4/IPv6 minimum w zakresie tras statycznych oraz protokołów RIP i OSPF
- k) policy Based Routing dla IPv4 oraz IPv6
- l) minimum 2000 wpisów multicast (S,G,V)
- m) minimum 4000 obsługiwanych sieci wirtualnych IEEE 802.1Q
- n) wsparcie dla ramek Jumbo Frames (min. 9K bajtów)

- o) obsługa Quality of Service (IEEE 802.1p, DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym)
- p) obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration)
- q) obsługa IGMP v1v2/v3 oraz IGMP v1/v2/v3 snooping
- r) obsługa protokołu PIM-SM
- s) Obsługa uwierzytelniania do sieci z wykorzystaniem:
 - protokołu IEEE 802.1x
 - formularza www
 - adresu MAC
- t) funkcjonalność elastycznego uwierzytelniania z możliwością wyboru kolejności stosowanych mechanizmów – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www)
- u) obsługa wielu sesji uwierzytelniania (min. 12) na jednym porcie (multiple supplicants)
- v) możliwość integracji funkcjonalności uwierzytelniania z systemem klasy NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z poziomu systemu NAC
- w) przydział sieci VLAN, ACL/QoS podczas autentykacji
- x) urządzenie musi wspierać profile bezpieczeństwa definiowane per użytkownik. Profil bezpieczeństwa oznacza połączenie:
 - definicji sieci VLAN,
 - reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,
 - realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,
 - realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.

- y) obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) wraz z funkcjonalnością per-command authentication
- z) bezpieczeństwo adresów MAC:
 - ograniczenie liczby MAC adresów na porcie
 - zatrzaśnięcie MAC adresu na porcie
 - możliwość wpisania statycznych MAC adresów na port/vlan
 - możliwość wyłączenia uczenia MAC adresów
- aa) zabezpieczenie przełącznika przed atakami DoS
 - Networks Ingress Filtering RFC 2267
 - SYN Attack Protection
 - zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
- bb) dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika)
- cc) obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation
- dd) obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard
- ee) obsługa redundancji routingu VRRP (RFC 2338) i VRRPv2 (RFC 3768)
- ff) obsługa protokołów drzewa rozpinającego (spanning tree) w zakresie STP, RSTP, MSTP, PVST+
- gg) obsługa protokołu MVRP
- hh) obsługa protokołu EAPS (RFC 3619), ERPS (ITU G.8032) lub równoważnego

- ii) obsługa Link Aggregation IEEE 802.3ad wraz z mechanizmem LACP
- jj) obsługa IEEE 802.3ah Ethernet OAM
- kk) obsługa mechanizmu MC-LAG/VSS/MLAG/IRF lub równoważnego umożliwiającego agregację połączeń do dwóch niezależnych przełączników. Urządzenia dołączające się do pary przełączników muszą widzieć je jako pojedyncze urządzenie z punktu widzenia warstwy L2. Nie dopuszcza się stosowania mechanizmów łączenia w stos jako równoważnych.
- ll) Sprzętowa obsługa sFlow lub protokołu równoważnego
- mm) Obsługa RMON (RFC 1757) i RMON2 (RFC 2021)
- nn) Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych)
- oo) Możliwość uruchamiania skryptów:
 - ręcznie
 - o określonym czasie lub co wskazany okres czasu
 - na podstawie wpisów w logu systemowym
- pp) Obsługa XML API poprzez Telnet/SSH i HTTP/HTTPS
- qq) Obsługa protokołu MACSEC (IEEE 802.1AE) na wszystkich portach urządzenia (zarówno porty miedziane jak i światłowodowe) – jeżeli funkcjonalność ta wymaga dodatkowych modułów lub licencji Zamawiający nie wymaga ich dostarczenia w ramach tego postępowania
- rr) usługi wirtualizacji warstwy L2 i L3 (Fabric Network)
 - przełącznik musi udostępniać możliwość wirtualizacji usług sieciowych w warstwie L2 i L3 modelu OSI.
 - przełącznik musi zapewniać „multi-tenancy” dla usług sieciowych zarówno w L2 jak i L3. Rozumiemy przez to

przypadek, w którym do przełącznika doprowadzone są nakładające się numery VLAN (vlan overlap) lub podsieci IP (subnet overlap). W takim przypadku przełącznik musi zapewniać izolację tego ruchu od siebie.

- przełącznik musi zapewniać usługi zwirtualizowane L2 i L3 w oparciu o standardowe protokoły sieciowe (SPB 802.1aq lub EVPN)
- przełącznik musi umożliwiać skonfigurowanie usług wirtualizacji w L2
- przełącznik musi umożliwiać obsługę usług multicast dla L2 jak i L3 bez konieczności używania protokołu PIM.
- przełącznik musi zapewniać możliwość zastosowania dowolnej topologii połączeń przy współpracy z innymi urządzeniami tworzącymi węzły sieci szkieletowej.
- przełącznik musi zapewniać możliwość dokładania nowych węzłów w sieci bez wpływu na już działające usługi sieciowe.

ss) modułarny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora

tt) możliwość monitorowania obciążenia CPU

uu) wbudowany port konsoli RJ45 oraz USB/Micro-USB

vv) zarządzanie za pomocą SSH/Telnet, SNMP v1/v2/v3, oraz systemu zarządzania dostarczonego przez producenta

ww) Obsługa SYSLOG z możliwością definiowania wielu serwerów

xx) wbudowany układ zasilania 230VAC

yy) przełącznik musi posiadać wbudowany zasilacz zapewniający budżet mocy dla technologii PoE na poziomie min. 370W

zz) dożywotnia gwarancja producenta (rozumiana co najmniej jako data zakończenia sprzedaży (EOS) + dodatkowe 5 lat) uwzględniająca:

- wymianę uszkodzonego urządzenia z wysyłką następnego dnia roboczego
- aktualizacje oprogramowania układowego (firmware)
- dostęp do bazy wiedzy oraz dokumentacji technicznej producenta

4.14.3. Dostarczyć jeden 48-portowy przełącznik sieciowy pozwalający na rozbudowę systemu łączności Monitoringu Prewencyjnego Wrocławia.

4.14.4. Minimalne wymagane parametry techniczne dla 48-portowych przełączników sieciowych:

- a) wysokość urządzenia 1U (rack 19")
- b) Przełącznik wyposażony w:
 - minimum 48 interfejsów 10/100/1000Base-T RJ45 PoE+
 - minimum 8 interfejsów 10GB Base-X SFP+
- c) możliwość łączenia do 8 urządzeń w stos zarządzany z pojedynczego adresu IP, połączenie pomiędzy poszczególnymi urządzeniami musi być możliwe z przepustowością minimum 40Gbps
- d) nieblokująca architektura o wydajności przełączania min. 256 Gbps i matrycy przełączającej z szybkością minimum 190 milionów pakietów na sekundę (Mpps)
- e) pojemność tablicy ARP: minimum 15000 wpisów
- f) pojemność tablicy adresów MAC: minimum 32 000 wpisów
- g) możliwość przypisania minimum 1000 ACL (sumarycznie wejściowe i wyjściowe)
- h) minimum 12000 wpisów w tablicy routingu IPv4
- i) minimum 6000 wpisów w tablicy routingu IPv6
- j) obsługa routingu IPv4/IPv6 minimum w zakresie tras statycznych oraz protokołów RIP i OSPF

- k) policy Based Routing dla IPv4 oraz IPv6
- l) minimum 4000 wpisów multicast (S,G,V)
- m) minimum 4000 obsługiwanych sieci wirtualnych IEEE 802.1Q
- n) wsparcie dla ramek Jumbo Frames (min. 9K bajtów)
- o) obsługa Quality of Service (IEEE 802.1p, DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym)
- p) obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration)
- q) obsługa IGMP v1v2/v3 oraz IGMP v1/v2/v3 snooping
- r) obsługa protokołu PIM-SM
- s) Obsługa uwierzytelniania do sieci z wykorzystaniem:
 - protokołu IEEE 802.1x
 - formularza www
 - adresu MAC
- t) funkcjonalność elastycznego uwierzytelniania z możliwością wyboru kolejności stosowanych mechanizmów – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www)
- u) obsługa wielu sesji uwierzytelniania (min. 12) na jednym porcie (multiple supplicants)
- v) możliwość integracji funkcjonalności uwierzytelniania z systemem klasy NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z poziomu systemu NAC
- w) przydział sieci VLAN, ACL/QoS podczas autentykacji
- x) urządzenie musi wspierać profile bezpieczeństwa definiowane per użytkownik. Profil bezpieczeństwa oznacza połączenie:
 - definicji sieci VLAN,

- reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,
 - realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,
 - realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.
- y) obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) wraz z funkcjonalnością per-command authentication
- z) bezpieczeństwo adresów MAC:
- ograniczenie liczby MAC adresów na porcie
 - zatrzaśnięcie MAC adresu na porcie
 - możliwość wpisania statycznych MAC adresów na port/vlan
 - możliwość wyłączenia uczenia MAC adresów
- aa) zabezpieczenie przełącznika przed atakami DoS
- Networks Ingress Filtering RFC 2267
 - SYN Attack Protection
 - zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
- bb) dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika)
- cc) obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation
- dd) obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard
- ee) obsługa redundancji routingu VRRP (RFC 2338) i VRRPv2 (RFC 3768)

- ff) obsługa protokołów drzewa rozpinającego (spanning tree) w zakresie STP, RSTP, MSTP, PVST+
- gg) obsługa protokołu MVRP
- hh) obsługa protokołu EAPS (RFC 3619), ERPS (ITU G.8032) lub równoważnego
- ii) obsługa Link Aggregation IEEE 802.3ad wraz z mechanizmem LACP
- jj) obsługa IEEE 802.3ah Ethernet OAM
- kk) obsługa mechanizmu MC-LAG/VSS/MLAG/IRF lub równoważnego umożliwiającego agregację połączeń do dwóch niezależnych przełączników. Urządzenia dołączające się do pary przełączników muszą widzieć je jako pojedyncze urządzenie z punktu widzenia warstwy L2. Nie dopuszcza się stosowania mechanizmów łączenia w stos jako równoważnych.
- ll) Sprzętowa obsługa sFlow lub protokołu równoważnego
- mm) Obsługa RMON (RFC 1757) i RMON2 (RFC 2021)
- nn) Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych)
- oo) Możliwość uruchamiania skryptów:
 - ręcznie
 - o określonym czasie lub co wskazany okres czasu
 - na podstawie wpisów w logu systemowym
- pp) Obsługa XML API poprzez Telnet/SSH i HTTP/HTTPS
- qq) Obsługa protokołu MACSEC (IEEE 802.1AE) na wszystkich portach urządzenia (zarówno porty miedziane jak i światłowodowe) – jeżeli funkcjonalność ta wymaga dodatkowych modułów lub licencji Zamawiający nie wymaga ich dostarczenia w ramach tego postępowania

rr) usługi wirtualizacji warstwy L2 i L3 (Fabric Network)

- przełącznik musi udostępniać możliwość wirtualizacji usług sieciowych w warstwie L2 i L3 modelu OSI.
- przełącznik musi zapewniać „multi-tenancy” dla usług sieciowych zarówno w L2 jak i L3. Rozumiemy przez to przypadek, w którym do przełącznika doprowadzone są nakładające się numery VLAN (vlan overlap) lub podsieci IP (subnet overlap). W takim przypadku przełącznik musi zapewniać izolację tego ruchu od siebie.
- przełącznik musi zapewniać usługi zwirtualizowane L2 i L3 w oparciu o standardowe protokoły sieciowe (SPB 802.1aq lub EVPN)
- przełącznik musi umożliwiać skonfigurowanie usług wirtualizacji w L2
- przełącznik musi umożliwiać obsługę usług multicast dla L2 jak i L3 bez konieczności używania protokołu PIM.
- przełącznik musi zapewniać możliwość zastosowania dowolnej topologii połączeń przy współpracy z innymi urządzeniami tworzącymi węzły sieci szkieletowej.
- przełącznik musi zapewniać możliwość dokładania nowych węzłów w sieci bez wpływu na już działające usługi sieciowe.

ss) modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora

tt) możliwość monitorowania obciążenia CPU

uu) wbudowany port konsoli RJ45 oraz USB/Micro-USB

vv) zarządzanie za pomocą SSH/Telnet, SNMP v1/v2/v3, oraz systemu zarządzania dostarczonego przez producenta

ww) Obsługa SYSLOG z możliwością definiowania wielu serwerów

xx) wbudowany układ zasilania 230VAC

- yy) przełącznik musi posiadać wbudowany zasilacz zapewniający budżet mocy dla technologii PoE na poziomie min. 740W
- zz) dożywotnia gwarancja producenta (rozumiana co najmniej jako data zakończenia sprzedaży (EOS) + dodatkowe 5 lat) uwzględniająca:
 - wymianę uszkodzonego urządzenia z wysyłką następnego dnia roboczego
 - aktualizacje oprogramowania układowego (firmware)
 - dostęp do bazy wiedzy oraz dokumentacji technicznej producenta

4.14.5. Rozbudować infrastrukturę zabezpieczenia brzegu sieci systemu łączności Monitoringu Prewencyjnego Wrocławia do odpowiedniego poziomu przepustowości i mocy obliczeniowej pozwalającej na płynne przesyłanie obrazu do systemu centralnego Genetec Security Center z wszystkich kamer monitoringu dostarczonych i zamontowanych w ramach przedmiotowego zadania.

4.14.6. Minimalne wymagane parametry techniczne dla infrastruktury zabezpieczenia brzegu sieci:

- a) Zapora sieciowa typu Next Generation Firewall (NGFW)
- b) Wbudowany mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku
- c) Wbudowana minimalna ilość interfejsów sieciowych:
 - 6 x 10 GbE SFP+
 - 2 x 10G/5G/2.5G/1G RJ45
 - 24 x RJ-45 Ethernet 10/100/1000

Każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa

- d) Wbudowane dodatkowe interfejsy:
 - 2 x USB 3.0

- 1 x konsola do zarządzania zaporą
 - 1 x RJ-45 Ethernet 10/100/1000 do zarządzania zaporą
- e) Wbudowany dysk M.2 o pojemności przynajmniej 128 GB z możliwością wymiany na większy
 - f) Możliwość przypisywania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa
 - g) Możliwość powiązywania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) umożliwiającą podniesienia wydajności połączeń oraz zapewniania redundancji
 - h) Możliwość tworzenia minimum 512 interfejsów logicznych VLAN (wsparcie dla standardu 802.1q)
 - i) Obsługa nielimitowanej ilości hostów podłączonych do sieci chronionej
 - j) Wydajność pozwalająca na minimum 5 000 000 jednocześnie obsługiwanych połączeń
 - k) Wydajność pozwalająca na minimum 228 000 nowych połączeń realizowanych w ciągu jednej sekundy
 - l) Wydajność pozwalająca na obsługę minimum 6 000 jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie)
 - m) Przepustowość urządzenia pracującego w trybie stateful firewall na poziomie nie mniejszym niż 28 Gbps (dla ramki 1518B zgodnie z RFC 2544)
 - n) Przepustowość urządzenia pracującego z włączonym mechanizmem IPS na poziomie nie mniejszym niż 17 Gbps
 - o) Przepustowość urządzenia pracującego jako koncentrator VPN na poziomie nie mniejszym niż 18 Gbps (szyfrowanie AES bez aktywnych usług UTM, zgodnie z RFC 2544)
 - p) Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez

buforowania i proxy i bez ograniczeń jeśli chodzi o wielkość skanowanych plików) na poziomie nie mniejszym niż 16 Gbps

- q) Wbudowany mechanizm inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem (administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron)
- r) Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS pozwalająca obsłużyć nie mniej niż 3 500 000 połączeń z przepustowością nie mniejszą niż 7 Gbps
- s) Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP
- t) Wbudowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site)
- u) Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa),
- v) Wbudowany mechanizm uwierzytelniania użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP
- w) Wsparcie dla Dynamicznego DNS tzw. DDNS
- x) Wbudowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne - Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony na które użytkownik wchodzi bezpośrednio)
- y) Administrator powinien mieć możliwość tworzenia różnych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak:

- wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron),
 - wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony,
 - wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki.
- z) Administrator powinien mieć możliwość tworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron dla danej kategorii np. 5 Mbps
- aa) Wbudowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL
- bb) Wbudowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPsec VPN
- cc) Wbudowany mechanizm uwierzytelniania bezprzewodowych stacji roboczych i użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci
- dd) Funkcjonalność pozwalająca na uruchomienie minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing oraz Failover (oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego)
- ee) Funkcjonalność pozwalająca na ograniczanie ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim

innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN)

- ff) Mechanizm kontroli dostępności zestawionych tuneli VPN
- gg) Wbudowany mechanizm zarządzania urządzeniem z wykorzystaniem protokołów: HTTP, HTTPS, SSH i SNMP
- hh) Możliwość konfiguracji oparta na pracy grupowej/obiektowej (polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do sieci internet powinna być tworzona według reguł opartych o grupy i obiekty)
- ii) Możliwość konfiguracji reguł dostępowych z wykorzystaniem trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić)
- jj) Wbudowany mechanizm NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego, oparty o reguły bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe)
- kk) Wbudowany mechanizm skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream – umożliwiający filtrowanie załączników poczty oraz skanowanie plików skompresowanych
- ll) Wbudowany mechanizm skanowania antyspyware
- mm) Wbudowany mechanizm IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www itp.
- nn) Wbudowany mechanizm IPS musi używać algorytmu szeregowego przetwarzania.

- oo) Wbudowany mechanizm zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex)
- pp) Wbudowane mechanizmy skanowania IPS / Antywirus / Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji
- qq) Bazy sygnatur mechanizmów IPS / Antywirus / Antyspyware muszą być aktualizowane co najmniej raz dziennie
- rr) Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur),
- ss) Administrator systemu musi mieć możliwość konfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur
- tt) Wbudowane systemy IPS / Antywirus / Antyspyware nie mogą posiadać ograniczeń związanych z rozmiarem skanowanych plików
- uu) Skanowanie IPS / Antywirus / Antyspyware musi być możliwe między strefami bezpieczeństwa
- vv) Wbudowane mechanizmy bezpieczeństwa muszą umożliwiać pełną kontrolę nad programami typu P2P, IM oraz aplikacjami multimedialnymi
- ww) Wsparcie mechanizmów QoS – priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p
- xx) Wsparcie dla komunikacji VoIP - pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń
- yy) Wbudowany mechanizm analizy behawioralnej (sandbox) obejmujący pliki wykonywalne PE, PDF, Office i aplikacje mobilne.

zz) Sandbox powinien działać z wykorzystaniem minimum 4 silników pochodzących od różnych producentów w celu zwiększenia skuteczności analizy sandbox - analiza powinna być wykonywana równolegle na wszystkich silnikach, a funkcjonalność nie może wymagać zakupu dodatkowych licencji

aaa) Wbudowana funkcjonalność SD-WAN bazująca minimum na poniższych parametrach: Jitter, Latency, Packet Loss - funkcjonalność nie może wymagać zakupu dodatkowych licencji

bbb) Wbudowany kontroler sieci bezprzewodowej kompatybilny z punktami dostępowymi pochodzącymi od tego samego producenta i pozwalający na obsługę do 512 takich punktów dostępowych sieci bezprzewodowej

ccc) Praca w trybie redundantnym w klastrze wysokiej dostępności (HA) – wymagane minimum dwa urządzenia o analogicznych parametrach (jedno urządzenie pracujące w trybie aktywnym oraz drugie urządzenie w trybie stand-by), oba urządzenia muszą synchronizować pomiędzy sobą stany sesji połączeń

ddd) Wykupione pełne wsparcie techniczne producenta w trybie 24x7 na okres minimum 36 miesięcy.

eee) Wymagane licencje:

- subskrypcja pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres 36 miesięcy.
- 2 licencje umożliwiające zestawienie połączeń typu client-site SSL VPN (komputer–urządzenie) z możliwością zwiększenia ich ilości do 1 500 lub więcej
- 2 000 licencji umożliwiających zestawienie połączeń typu client-site IPSec VPN (komputer–urządzenie) z możliwością zwiększenia ich ilości do 4 000 lub więcej

4.14.7. Czynności montażowe i rozruchowe:

a) montaż w wyznaczonym miejscu w szafie typu Rack 19"

- b) aktywacja urządzeń
- c) aktualizacji do najnowszej dostępnej wersji
- d) utworzenie klastra wysokiej dostępności HA
- e) włączenie dostępu do interfejsu zarządzania (np. interfejs WEB, dostęp poprzez SSH)
- f) podłączenie urządzenia do infrastruktury klienta

4.14.8. Czynności konfiguracyjne:

- a) utworzenie stref sieciowych (ZONE)
- b) utworzenie interfejsów sieciowych (VLAN)
- c) utworzenie reguł bezpieczeństwa (ACL)
- d) utworzenie reguł NAT
- e) utworzenie wpisów w tablicy routingu
- f) włączenie mechanizmów ochronnych (m.in. antywirus, antyspyware, IPS, capture ATP dla ruchu wejściowego, oraz wyjściowego)
- g) uruchomienie deszyfracji ruchu na wybranych serwerach
- h) zabezpieczenie dostępu do urządzenia poprzez zmianę domyślnego hasła dla administratora lokalnego
- i) utworzenie użytkowników lokalnych dla każdego z administratorów
- j) podłączenie bazy LDAP z użytkownikami
- k) konfiguracja wysyłania wpisów LOG na zewnętrzny serwer SYSLOG
- l) włączenie monitoringu poprzez SNMP
- m) konfiguracja komunikacji MULTICAST w warstwie L3

4.14.9. Testy funkcjonalne i użytkowe:

- a) przeprowadzenie analizy obciążenia urządzenia.
- b) przeprowadzenie analizy poprawności działania reguł ACL

- c) przeprowadzenie analizy poprawności działania reguł NAT
- d) przeprowadzenie analizy działania serwisów bezpieczeństwa
- e) przeprowadzenie testów poprawności działania.
- f) weryfikacja otwartych portów na urządzeniu UTM
- g) weryfikacja poprawności działania klastra HA
- h) wykonanie analizy pakietów komunikacji wybranych hostów przez klienta

4.14.10. Szkolenia i instruktaż techniczny:

- a) przeprowadzenie zaawansowanego szkolenia z obsługi urządzenia dla administratorów
- b) zapoznanie administratorów z najczęstszymi przypadkami problemów wraz z metodami rozwiązywania problemów
- c) przygotowanie i dostarczenie dokumentacji powdrożeniowej wraz z instrukcją obsługi urządzenia w języku Polskim.

4.15. W zakresie włączenia nowych kamer do systemu VMS Genetec Security Center należy:

4.15.1. Dostarczyć wszelkie wymagane licencje, aby włączyć wszystkie zamontowane urządzenia do centralnego systemu posiadanego przez Zamawiającego tj. Genetec Security Center w najnowszej dostępnej wersji zgodnie z aktualnym SUP (Software Upgrade Plan) producenta tego oprogramowania.

4.15.2. Wykonać pełną konfigurację urządzeń do pracy w systemie Genetec Security Center.

2. Wymagania techniczne i funkcjonalne dla kamer monitoringu oraz głośników sieciowych:

2.1. W ramach realizacji przedmiotowego zadania należy stosować kamery PTZ typu AXIS P5676-LE lub równoważne o parametrach technicznych nie gorszych niż:

- a) rozmiar przetwornika obrazu: nie mniejszy niż 1/3"

- b) rozdzielczość obrazu: minimum 4MP 2688x1512
- c) minimum 30-krotny zoom optyczny
- d) wbudowana funkcja automatycznego ustawiania ostrości
- e) maksymalna dostępna poklatkowość dla pełnej rozdzielczości obrazu: nie mniej niż 25 fps
- f) wbudowany mechanizm optymalizacji strumienia wideo
- g) kompresja obrazu: MJPEG, H.264, H.265
- h) wbudowany oświetlacz podczerwieni
- i) wbudowany mechanizm sztucznej inteligencji pozwalający na wykrywanie i klasyfikację obiektów z podziałem na ludzi i pojazdy
- j) zasilanie w standardzie PoE: IEEE 802.3at lub IEEE 802.3bt
- k) zgodność ze standardem IEEE 802.1X
- l) zgodność ze standardem infrastruktury klucza publicznego z certyfikatami X.509
- m) wbudowane funkcje bezpieczeństwa: ochrona hasłem, podpisane oprogramowanie, ochrona przed atakami brute force, wbudowany moduł kryptograficzny zgodny z FIPS 140-2, 256-bitowe szyfrowanie kart pamięci
- n) możliwość pracy w warunkach temperaturowych z zakresu nie mniejszego niż -30 do +50°C
- o) odporność na warunki atmosferyczne na poziomie minimum IP65
- p) odporność na uszkodzenia mechaniczne na poziomie minimum IK08 dla montażu od 3m nad poziomem gruntu włącznie lub minimum IK10 dla montażu poniżej 3m
- q) 5-letnia gwarancja producenta

2.2. W ramach realizacji przedmiotowego zadania należy stosować kamery wielokierunkowe typu AXIS P3737-PLE lub równoważne o parametrach technicznych nie gorszych niż:

- a) wbudowane minimum cztery przetworniki
- b) możliwość niezależnej regulacji położenia każdego z przetworników/obiektów (panoramowanie, pochylenie, obrót, skręt)
- c) rozmiar przetwornika obrazu: nie mniejszy niż 1/2.7"
- d) rozdzielczość obrazu: minimum 5MP 2592x1944
- e) wbudowana funkcja zdalnego ustawiania ostrości
- f) maksymalna dostępna poklatkowość dla pełnej rozdzielczości obrazu: nie mniej niż 20 fps
- g) wbudowany mechanizm optymalizacji strumienia wideo
- h) kompresja obrazu: MJPEG, H.264, H.265
- i) wbudowany mechanizm sztucznej inteligencji pozwalający na wykrywanie i klasyfikację obiektów z podziałem na ludzi i pojazdy
- j) zasilanie w standardzie PoE: IEEE 802.3at lub IEEE 802.3bt
- k) zgodność ze standardem IEEE 802.1X
- l) zgodność ze standardem infrastruktury klucza publicznego z certyfikatami X.509
- m) wbudowane funkcje bezpieczeństwa: ochrona hasłem, podpisane oprogramowanie, ochrona przed atakami brute force, wbudowany moduł kryptograficzny zgodny z FIPS 140-2, 256-bitowe szyfrowanie kart pamięci
- n) możliwość pracy w warunkach temperaturowych z zakresu nie mniejszego niż -30 do +50°C
- o) odporność na warunki atmosferyczne na poziomie minimum IP65
- p) odporność na uszkodzenia mechaniczne na poziomie minimum IK08 dla montażu od 3m nad poziomem gruntu włącznie lub minimum IK10 dla montażu
- q) 5-letnia gwarancja producenta

2.3. W ramach realizacji przedmiotowego zadania należy stosować kamery dwukierunkowe typu AXIS P4707-PLVE lub równoważne o parametrach technicznych nie gorszych niż:

- a) wbudowane dwa przetworniki
- b) możliwość niezależnej regulacji położenia każdego z przetworników/obiektów (panoramowanie, pochylenie, obrót)
- c) rozmiar przetwornika obrazu: nie mniejszy niż 1/2.7"
- d) rozdzielczość obrazu: minimum 5MP 2592x1944
- e) wbudowana funkcja zdalnego ustawiania ostrości
- f) maksymalna dostępna poklatkowość dla pełnej rozdzielczości obrazu: nie mniej niż 20 fps
- g) wbudowany mechanizm optymalizacji strumienia wideo
- h) kompresja obrazu: MJPEG, H.264, H.265
- i) wbudowany mechanizm sztucznej inteligencji pozwalający na wykrywanie i klasyfikację obiektów z podziałem na ludzi i pojazdy
- j) zasilanie w standardzie PoE: IEEE 802.3at lub IEEE 802.3bt
- k) zgodność ze standardem IEEE 802.1X
- l) zgodność ze standardem infrastruktury klucza publicznego z certyfikatami X.509
- m) wbudowane funkcje bezpieczeństwa: ochrona hasłem, podpisane oprogramowanie, ochrona przed atakami brute force, wbudowany moduł kryptograficzny zgodny z FIPS 140-2, 256-bitowe szyfrowanie kart pamięci
- n) możliwość pracy w warunkach temperaturowych z zakresu nie mniejszego niż -30 do +50°C
- o) odporność na warunki atmosferyczne na poziomie minimum IP65

- p) odporność na uszkodzenia mechaniczne na poziomie minimum IK08 dla montażu od 3m nad poziomem gruntu włącznie lub minimum IK10 dla montażu
- q) 5-letnia gwarancja producenta

2.4. W ramach realizacji przedmiotowego zadania należy stosować kamery stałopozycyjne wysokiej rozdzielczości typu AXIS P3267-LVE lub równoważne o parametrach technicznych nie gorszych niż:

- a) rozmiar przetwornika obrazu: nie mniejszy niż 1/2.7"
- b) rozdzielczość obrazu: minimum 5MP 2592x1944
- c) wbudowana funkcja zdalnego ustawiania ostrości
- d) maksymalna dostępna poklatkowość dla pełnej rozdzielczości obrazu: nie mniej niż 25 fps
- e) wbudowany mechanizm optymalizacji strumienia wideo
- f) kompresja obrazu: MJPEG, H.264, H.265
- g) wbudowany mechanizm sztucznej inteligencji pozwalający na wykrywanie i klasyfikację obiektów z podziałem na ludzi i pojazdy
- h) zasilanie w standardzie PoE: IEEE 802.3af lub IEEE 802.3at
- i) zgodność ze standardem IEEE 802.1X
- j) zgodność ze standardem infrastruktury klucza publicznego z certyfikatami X.509
- k) wbudowane funkcje bezpieczeństwa: ochrona hasłem, podpisane oprogramowanie, ochrona przed atakami brute force, wbudowany moduł kryptograficzny zgodny z FIPS 140-2, 256-bitowe szyfrowanie kart pamięci
- l) możliwość pracy w warunkach temperaturowych z zakresu nie mniejszego niż -30 do +50°C
- m) odporność na warunki atmosferyczne na poziomie minimum IP65

- n) odporność na uszkodzenia mechaniczne na poziomie minimum IK08 dla montażu od 3m nad poziomem gruntu włącznie lub minimum IK10 dla montażu
- o) 5-letnia gwarancja producenta

2.5. W ramach realizacji przedmiotowego zadania należy stosować głośniki sieciowe typu AXIS C1310-E Mk II lub równoważne o parametrach technicznych nie gorszych niż:

- a) obudowa tubowa
- b) maksymalny poziom ciśnienie dźwięku nie mniejszy niż 120 dB
- c) spektrum propagacji dźwięku w poziomie nie mniejsze niż 70°
- d) spektrum propagacji dźwięku w poziomie nie mniejsze niż 100°
- e) odtwarzanie nagrań fonicznych
- f) obsługa nagrań w formatach WAV, MP3
- g) wyzwalanie zdarzeń (wejścia, wyjścia)
- h) zasilanie w standardzie PoE: IEEE 802.3af lub IEEE 802.3at
- i) zgodność ze standardem IEEE 802.1X
- j) zgodność ze standardem infrastruktury klucza publicznego z certyfikatami X.509
- k) wbudowane funkcje bezpieczeństwa: ochrona hasłem, podpisane oprogramowanie, ochrona przed atakami brute force
- l) możliwość pracy w warunkach temperaturowych z zakresu nie mniejszego niż -30 do +50°C
- m) odporność na warunki atmosferyczne na poziomie minimum IP65
- n) 5-letnia gwarancja producenta

3. Wymagania techniczne i funkcjonalne dla urządzeń systemu łączności radiowej LMDS:

3.1. Istniejąca radiowa sieć teletransmisyjna Gminy Wrocław:

- a) Istniejąca radiowa sieć teletransmisyjna we Wrocławiu oparta jest o rozwiązania radiowe Intracom Telecom™, pracujące w licencjonowanych pasmach pracy LMDS.
- b) Ze względu na wycofanie z produkcji systemów WiBAS-HCS oraz WiBAS-C, wszystkie dostarczane urządzenia łączności radiowej muszą być w pełni kompatybilne z systemem WiBAS-OSDR funkcjonującym w systemie łączności radiowej użytkowanym przez Zamawiającego.

3.2. System zarządzania:

- a) Zamawiający wykorzystuje obecnie system zarządzania uniMS z licencjami na linie radiowe serii OmniBAS i StreetNode oraz system LMDS OSDR-WiBAS Intracom Telecom.
- b) W ramach realizacji zamówienia należy dostarczyć wszelkie niezbędne licencje wymagane do włączenia i konfiguracji nowych urządzeń dostarczanych w ramach przedmiotowego Zamówienia.

3.3. Urządzenia łączności radiowej LMDS:

- a) Urządzenia zewnętrzne muszą posiadać budowę typu outdoor.
- b) Urządzenia muszą pracować w paśmie LMDS ETSI 28 GHz.
- c) Urządzenia muszą umożliwiać pracę w kanałach z zakresów: kanały 21÷32 z planu 28A28 oraz kanały 11÷16 z planu 28A56.
- d) Urządzenia muszą umożliwiać pracę sektorową, z wykorzystaniem szerokości kanału 28MHz oraz 56MHz w ramach pojedynczego modułu.
- e) Wymagana zagregowana przepustowość radiowa dla stacji na poziomie nie niższym niż 1 Gbps.
- f) Moc nadajnika po stronie stacji terminalowych dla pasma 28 MHz nie może być gorsza niż 17 dBm.
- g) Zysk anteny stacji terminalowej dla anten parabolicznych powinien być nie gorszy niż 35 dBi dla anten 0.3 m oraz nie

gorszy niż 40 dBi
dla anten 0.6 m.

- h) Zysk anteny stacji sektorowej powinien być nie gorszy niż 15dBi w przypadku anteny 90 stopni oraz nie gorszy niż 12dBi w przypadku anteny 180stopni
- i) Każdy terminal radiowy powinien posiadać min. 2 porty dostępowe
w tym minimum 1 port Gigabit Ethernet (elektryczny lub optyczny).
- j) System powinien wspierać minimum następujące protokoły łączności sieciowej: IEEE 802.1ad oraz IEEE 802.1Q (VLAN).
- k) Terminal radiowy powinien posiadać zaimplementowane funkcje Ethernet QoS.
- l) Urządzenie powinno posiadać zaimplementowane mechanizmy bezpieczeństwa MAC Security, Port Flooding, MAC Learning, Storm Control, Split Horizon.
- m) Urządzenia powinny cechować się budową kompaktową, a waga pojedynczego urządzenia łącznie z anteną i uchwytem nie powinna przekraczać 5 kg.
- n) Obudowa urządzeń montowanych w warunkach zewnętrznych powinna posiadać klasę szczelności na poziomie nie mniejszym niż IP67.
- o) Urządzenia powinny być kompatybilne z systemem zarządzania uniMS, posiadanym przez Zamawiającego.

3.4. Połączenia lokalne należy wykonywać za pomocą rozwiązań systemowych typu Street Node LMDS 28 GHz.

3.5. Wykonawca ma obowiązek wykazania kompatybilności urządzeń z systemami WIBAS-OSDR oraz uniMS przed zainstalowaniem urządzeń łączności radiowej w terenie.

- 3.6. Wykonawca przed uruchomieniem łączności radiowej zobowiązany jest do przygotowania wszelkich niezbędnych dokumentów wraz z załącznikami w celu realizacji niezbędnych czynności administracyjnych w Urzędzie Komunikacji Elektronicznej.
- 3.7. Zamawiający wymaga, aby wykonawca dostarczył wraz z dostarczaniem urządzeniami łączności radiowej LMDS wszelkie niezbędne licencje wymagane do uruchomienia i zarządzania linkami radiowymi wykonanymi w ramach przedmiotowego zamówienia.
- 3.8. Zamawiający wymaga, aby wszystkie parametry techniczne urządzeń radiowych oraz ich cechy funkcjonalno-użytkowe wynikające z treści SWZ oraz OPZ były wdrożone i dostępne na rynku (w sprzedaży) na dzień składania ofert.