

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Określenie przedmiotu i zakresu zamówienia:

Przedmiotem zamówienia jest dostawa licencji i uruchomienie nowoczesnych mechanizmów inteligencji, zarządzania oraz analizy materiału wideo w systemie Monitoringu Prewencyjnego Wrocławia.

2. Wymagania ogólne:

- 2.1. Zamawiający wymaga, aby zamówienie było zrealizowane kompletnie, w pełnym zakresie i zgodnie z wymaganiami Zamawiającego określonymi w niniejszym OPZ, SIWZ oraz warunkami umowy.
- 2.2. Zamawiający wymaga, aby zamówienie było wykonane z należyłą 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. Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów i być przeznaczone dla tego projektu – do oferty należy dołączyć odpowiednie oświadczenie Wykonawcy.
- 2.4. Zamawiający wymaga aby oferowane przez Wykonawcę urządzenia oraz oprogramowanie były jednorodne (tj. zakazuje się zaoferowania a następnie dostarczania różnych modeli urządzeń i oprogramowania, elementy muszą być tożsame w ramach modelu).
- 2.5. Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 9 miesięcy przed ich dostarczeniem) oraz by nie były używane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem).
- 2.6. Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowiło naruszenia majątkowych praw autorskich osób trzecich.
- 2.7. Zamawiający zastrzega sobie możliwość wystąpienia z wnioskiem do Wykonawcy o wskazanie w publicznie dostępnej dokumentacji producenta (np. strona www z dokumentacją techniczną opisującą dane urządzenie/oprogramowanie) potwierdzenia spełnienia wymogów. Nie spełnienie tego warunku w ciągu 3 dni roboczych od dnia otrzymania wniosku będzie skutkowało odrzuceniem oferty.
- 2.8. Zamawiający zastrzega sobie prawo zażądania testów poszczególnych funkcjonalności przed wyborem oferty. Na żądanie Zamawiającego Wykonawca zobowiązany będzie do dostarczenia w ciągu 3 dni roboczych od wezwania urządzeń/oprogramowania celem przeprowadzenia testów. W przypadku oprogramowania Wykonawca wykona instalację i konfigurację na udostępnionej przez Zamawiającego stacji roboczej.
- 2.9. Zamawiający zastrzega sobie możliwość zwrócenia się do producentów oferowanych produktów o potwierdzenie, że sprzęt i licencje nie były przeznaczone dla innego odbior-

cy (w także do przekazania producentowi niezbędnych danych umożliwiających weryfikację) jak również zastrzega sobie prawo sprawdzenia u producentów warunków gwarancyjnych i wsparcia na oferowane rozwiązanie.

2.10. Zgodnie z Prawem Zamówień Publicznych zezwala się na dobór urządzeń 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 oraz przedłożyć wykaz oferowanych materiałów.

3. Organizacja prac i etapowanie zadań:

3.1. Zadanie zostało podzielone na dwa etapy:

3.1.1. Etap 1 - Dostawa wymaganych licencji:

- a) W ramach Etapu 1 Wykonawca zobowiązany jest do dostawy wszystkich wymaganych licencji zgodnie z OPZ pkt 4.1.
- b) Przed dostarczeniem licencji Wykonawca dokona wszelkich niezbędnych analiz przy udziale Zamawiającego, aby odpowiednio dobrać zakres oraz typ dostarczanych licencji z uwzględnieniem wszelkich wymagań funkcjonalnych i technicznych opisanych w OPZ.
- c) W trakcie prowadzonych analiz Wykonawca zobowiązany jest na wezwanie Zamawiającego do uruchomienia testowej instancji systemu w celu wykazania spełniania wymagań opisanych w OPZ w przypadku wystąpienia jakichkolwiek wątpliwości po stronie Zamawiającego.

3.1.2. Etap 2 - Uruchomienie Zunifikowanej Platformy Bezpieczeństwa wraz z zaawansowanymi mechanizmami inteligencji, zarządzania oraz analizy materiału wideo:

- a) W ramach Etapu 2 Wykonawca zobowiązany jest do uruchomienia Zunifikowanej Platformy Bezpieczeństwa z wykorzystaniem licencji dostarczonych w Etapie 1.
- b) W pierwszej kolejności Wykonawca uruchomi bazową instancję Zunifikowanej Platformy Bezpieczeństwa z wykorzystaniem urządzeń serwerowych posiadanych przez Zamawiającego.
- c) Po uruchomieniu części serwerowej Zunifikowanej Platformy Bezpieczeństwa Wykonawca dokona konfiguracji macierzy oraz włączenia kamer monitoringu w celu realizacji podstawowych funkcji systemu w zakresie zarządzania materiałem wideo (VMS). Na tym etapie prac należy wykorzystać istniejące zasoby serwerowo-macierzowe posiadane przez Zamawiającego.
- d) Po uruchomieniu funkcjonalności zarządzania materiałem wideo (VMS) dla wszystkich istniejących kamer monitoringu wizyjnego Wykonawca dokona wygaszenia dotychczasowego systemu we współpracy z Zamawiającym.
- e) Wykonawca w trakcie procedury wygaszania dotychczasowego systemu dokona równoległego uruchomienia mechanizmów zaawansowanej inteligencji oraz analityki.
- f) Przed zakończeniem prac Wykonawca przeprowadzi szkolenie dla administratorów systemu oraz operatorów systemu zgodnie z zapisami OPZ pkt 7.
- g) Wraz ze zgłoszeniem przedmiotu Zamówienia do odbioru Wykonawca dostarczy certyfikat/licencję potwierdzającą obowiązywanie wsparcia SMA dla uruchomionej Zunifikowanej Platformy Bezpieczeństwa.

- 3.2. Realizacja poszczególnych etapów zadania musi odbywać się chronologicznie w terminach wskazanych w Umowie.
- 3.3. Zamawiający zastrzega sobie prawo do wyznaczenia kilkuosobowego zespołu technicznego, który będzie brał udział w procesie implementacji, nabywając doświadczenia niezbędnego przy późniejszej eksploatacji systemu.

4. Wymagania ilościowe:

- 4.1. Wykonawca zobowiązany jest dostarczyć Zamawiającemu Zunifikowaną Platformę Bezpieczeństwa umożliwiającą zarządzania oraz analizę materiału wideo z wykorzystaniem wbudowanych mechanizmów inteligencji, zawierający minimum:
- a) 1 licencję serwerową Zunifikowanej Platformy Bezpieczeństwa stanowiącą podstawę do uruchomienia wszystkich kluczowych elementów i funkcjonalności systemu.
 - b) 1 licencję systemu Zarządzania Materiałem Wideo (VMS)
 - c) 1 licencję systemu Kontroli Dostępu (ACS)
 - d) 1 licencję systemu Automatycznego Rozpoznawania Tablic Rejestracyjnych (ALPR)
 - e) 1 licencję umożliwiającą połączenie nadrzędne z systemem zewnętrznym (Federacja)
 - f) 250 licencji kamerowych obejmujących połączenie bazowe
 - g) 250 licencji kamerowych obejmujących połączenie fail-over
 - h) 50 licencji zaawansowanej analityki dla kamer stałopozycyjnych
 - i) 2 licencje kamerowe ALPR
 - j) 30 licencji dla stanowisk operatorskich
 - k) 5 licencji dla terminali mobilnych
- 4.2. Każda z licencji wskazanych w OPZ pkt. 4.1 może się składać z licencji podstawowych i ich rozszerzeń, poszczególne licencje mogą się również zawierać w licencji zbiorczej, pod warunkiem łącznego spełniania wymaganych funkcjonalności i parametrów technicznych.

5. Wymagania funkcjonalne:

5.1. Platforma Bezpieczeństwa:

- 5.1.1. Zamawiający wymaga, aby dostarczone rozwiązanie było zunifikowanym systemem, który pełni rolę Platformy Bezpieczeństwa.
- 5.1.2. Jako zunifikowaną Platformę Bezpieczeństwa należy rozumieć oprogramowanie serwerowe oraz klienckie posiadające wbudowane wszystkie wymagane kluczowe funkcjonalności oraz narzędzia, bez konieczności wykorzystywania rozwiązań pomocniczych pochodzących od innych dostawców i producentów.
- 5.1.3. Wykorzystywanie rozwiązań pomocniczych pochodzących od innych dostawców i producentów dopuszczalne jest wyłącznie dla funkcjonalności dodatkowych.
- 5.1.4. Do kluczowych funkcjonalności należą minimum:
- a) Zarządzanie Materiałem Wideo (VMS)
 - b) System Kontroli Dostępu (ACS)
 - c) Automatyczne Rozpoznawanie Tablic Rejestracyjnych (ALPR)

5.1.5. Zamawiający dopuszcza, aby kluczowe funkcjonalności Platformy Bezpieczeństwa opisane w OPZ pkt 5.1.4 mogły być licencjonowane łącznie lub oddzielnie w ramach licencji serwerowej.

5.1.6. Do kluczowych narzędzi należą minimum:

- a) Dynamiczne mapy graficzne
- b) Zaawansowana analityka wideo i mechanizmy inteligencji
- c) Aplikacja Klientka PC
- d) Webowa Aplikacja Klientka (tzw. web-client)
- e) Mobilna Aplikacja Klientka (dostępna na smartfony i tablety)
- f) Federacje

5.1.7. Platforma Bezpieczeństwa musi posiadać zdolność działania jako system klasy PSIM (*Physical Security Information Management*) pozwalający na tworzenie rozbudowanych, wieloparametrowych i wielostopniowych procedur oraz algorytmów decyzyjnych, w których każdy krok może podlegać oddzielnej weryfikacji, autoryzacji lub akceptacji, służący jako narzędzie wspierania decyzji i korelowania zdarzeń.

5.1.8. Dostęp do Platformy Bezpieczeństwa z poziomu operatora systemu musi być realizowany poprzez Aplikację Klientką posiadającą wbudowany Pulpit Sterowniczy.

5.1.9. Jako aplikację kliencką należy rozumieć podstawowe narzędzie pracy operatora systemu, dostępne jako rozwiązanie desktopowe na systemy operacyjne z rodziny Microsoft Windows (Windows 7 Professional 64-bit PL oraz Windows 10 Professional 64-bit PL).

5.2. Kluczowe funkcje Platformy Bezpieczeństwa:

5.2.1. Zarządzanie Materiałem Wideo (VMS)

- a) Funkcjonalność VMS musi stanowić integralną część Platformy Bezpieczeństwa. Jeśli podlega odrębnemu licencjonowaniu Wykonawca zobowiązany jest taką licencję dostarczyć w ramach licencji serwerowej wskazanej w OPZ pkt 4.1.
- b) Dostarczona licencja VMS musi:
 - być wieczysta, tzn. nieograniczona w czasie
 - oferować bieżące aktualizacje zgodnie z planem aktualizacji oprogramowania przez 3 lata od momentu uruchomienia systemu (Zamawiający dopuszcza, aby aktualizacje podlegały osobnemu licencjonowaniu na zasadzie subskrypcji czasowej)
 - umożliwiać obsługę nieograniczonej ilości strumieni z kamer (Zamawiający wymaga dostarczenia licencji na 250 strumieni z kamer)
 - umożliwiać obsługę nieograniczonej ilości stanowisk operatorskich (Zamawiający wymaga dostarczenia licencji na 30 stanowisk operatorskich)
 - umożliwiać pełnienie roli nadrzędnej instancji w strukturze federacji między systemami VMS opartymi na tej samej Platformie Bezpieczeństwa
- c) VMS musi posiadać zaimplementowane inteligentne strumieniowanie i zarządzaniu przepustowością w celu optymalnego wykorzystania zasobów sieciowych i zabezpieczenia sieci przed nadmiernym przeciążeniem m.in. musi posiadać mechanizm automatycznego wyboru wielkość i jakość strumienia, odpowiadającą wielkości kafelka wideo aktualnie wyświetlanego na siatce obrazu.

Inteligentne strumieniowanie musi wykorzystywać minimum 5 strumieni wideo różnej wielkości i jakości strumienia.

- d) VMS musi posiadać wbudowane mechanizmy przełączania awaryjnego i redundancji w celu zapewnienia wysokiej niezawodności i ochrony przed awarią.
- e) Producent oprogramowania musi udostępniać na swojej ogólnodostępnej stronie internetowej wykaz urządzeń, które zostały sprawdzone pod względem kompatybilności z dostarczoną Platformą Bezpieczeństwa. Wykaz kompatybilnych urządzeń musi również uwzględniać aspekty cyber bezpieczeństwa.
- f) VMS musi posiadać mechanizm buforowania strumieni wideo (na żywo oraz archiwalnych) w pamięci podręcznej cache znajdującej się na stacji klienckiej, która pozwala na szybkie przeglądanie zapisanego materiału bezpośrednio przed zdarzeniem oraz w trakcie gromadzenia materiału dowodowego bez konieczności odpytywania serwera.
- g) VMS musi umożliwiać wykorzystywanie klawiatur i joysticków na stanowiskach operatorskich do sterowania kamerami oraz zarządzania systemem VMS np. poprzez wybór kamery, odtwarzanie materiału wideo (start, pauza, stop, przewijanie do przodu, przewijanie do tyłu) itp.
- h) VMS musi umożliwiać szybkie przeszukiwanie zapisanego materiału wizyjnego we wskazanym przez operatora obszarze.
- i) VMS musi umożliwiać powiązanie zdarzeń rozpoznawania tablic rejestracyjnych z dowolnie wybranymi kamerami monitoringu.
- j) VMS musi zapewniać wykorzystywanie modułu dynamicznych map graficznych.
- k) VMS musi posiadać funkcjonalność wykorzystywania procesora graficznego (GPU) stacji roboczej do renderowania obrazu wideo dla stacji roboczych wyposażonych karty graficzne z rodziny NVIDIA o architekturze Maxwell lub nowszej.
- l) VMS musi posiadać zaimplementowane szyfrowanie strumieni wideo zgodnie z algorytmem AES-128.
- m) VMS musi posiadać zdolność wykorzystywania strumieni wideo z kodowaniem MJPEG, H.264 oraz H.265.

5.2.2. System Kontroli Dostępu (ACS)

- a) Funkcjonalność ACS musi stanowić integralną część Platformy Bezpieczeństwa. Jeśli podlega odrębnemu licencjonowaniu Wykonawca zobowiązany jest taką licencję dostarczyć w ramach licencji serwerowej wskazanej w OPZ pkt 4.1.
- b) Dostarczona licencja ACS musi:
 - być wieczysta, tzn. nieograniczona w czasie
 - umożliwiać obsługę minimum 64 czytników kart RFID
 - umożliwiać obsługę minimum 5 stanowisk operatorskich
- c) ACS musi posiadać wbudowane narzędzie do projektowania nadruków na kartach RFID umożliwiające tworzenie nadruków składających się z napisów, grafik (w formatach: BMP, JPG, GIF, PNG) oraz kodów kreskowych (o kodowaniu: Code 39, Extended Code 39 oraz Interleaved 2 of 5).
- d) ACS musi umożliwiać tworzenie scenariuszy poprzez wykorzystanie funkcji:

- "antipassback" - uniemożliwiającej ponowne otwarcie danych drzwi w zadeklarowanym odstępie czasu, bądź bez uprzedniego przejścia do kolejnego kontrolera drzwiowego,
- "two-man rule" - uniemożliwiającej poruszanie się po obiekcie bez nadzoru przez cały czas pobytu w obiekcie,
- "first-person-in" - uniemożliwiającej wejście do określonych stref w obiekcie, jeśli w danej strefie nie przebywają określone osoby uprawnione.

5.2.3. Automatyczne Rozpoznawanie Tablic Rejestracyjnych (ALPR)

- Funkcjonalność ALPR musi stanowić integralną część Platformy Bezpieczeństwa. Jeśli podlega odrębnemu licencjonowaniu Wykonawca zobowiązany jest taką licencję dostarczyć w ramach licencji serwerowej wskazanej w OPZ pkt 4.1.
- Dostarczona licencja ALPR musi:
 - być wieczysta, tzn. nieograniczona w czasie
 - oferować bieżące aktualizacje zgodnie z planem aktualizacji oprogramowania przez minimum 3 lata od momentu uruchomienia systemu (Zamawiający dopuszcza, aby aktualizacje podlegały osobnemu licencjonowaniu na zasadzie subskrypcji czasowej)
 - umożliwiać obsługę minimum 2 strumieni z kamer IP, które będą obsługiwane na poziomie serwera (Zamawiający wymaga dostarczenia i uruchomienia 2 tego typu licencji)
 - umożliwiać obsługę minimum 5 stanowisk operatorskich
- ALPR musi posiadać wbudowany mechanizm analizy i wyszukiwania podobnych skojarzeń z listy pojazdów, który ma za zadanie ułatwiać operatorom systemu obsługę zdarzeń ALPR w przypadku wystąpienia błędnych odczytów spowodowanych np. zabrudzeniem tablicy rejestracyjnej lub odczytów w złych warunkach pogodowych.
- ALPR musi umożliwiać na poziomie serwera analizę strumieni wideo z kamer IP włączonych do systemu VMS zapewniając wszystkie wymagane funkcjonalności systemu.
- ALPR musi umożliwiać wykorzystywanie dedykowanych kamer ALPR pozwalających na odczyty na poziomie do 5000 pojazdów na minutę, poruszających się z prędkościami do 200 km/h lub więcej.
- ALPR musi umożliwiać sterowanie urządzeniami zewnętrznymi typu: szlabany, bramy garażowe, słupki przeszkodowe itp. na podstawie odczytów z kamer i nadawanych uprawnień w systemie ALPR.
- ALPR musi umożliwiać tworzenie alarmów dla operatorów systemu w przypadku wykrycia pojazdów zdefiniowanych np. jako pojazdy wymagające weryfikacji podczas wjazdu na teren obiektu lub pojawienie się na terenie obiektu osób o statusie VIP.

5.3. Kluczowe narzędzia Platformy Bezpieczeństwa

5.3.1. Dynamiczne Mapy Graficzne

- Zamawiający wymaga, aby narzędzie Dynamicznych Map Graficznych zostało dostarczone w ramach zadania i było dostępne bez ograniczeń czasowych dla każdego stanowiska operatorskiego Platformy Bezpieczeństwa.

- b) Narzędzie musi współpracować z systemami Zarządzanie Materiałem Wideo (VMS), Kontroli Dostępu (ACS) oraz Automatycznego Rozpoznawania Tablic Rejestracyjnych (ALPR).
- c) Narzędzie musi pozwalać na wizualizację i kontrolę elementów systemu m.in. takich jak czujniki, elementy wykonawcze, przejścia, a w szczególności kamery monitoringu wizyjnego.
- d) Narzędzie musi obsługiwać m.in. takie formaty plików jak: PDF, JPG, PNG, WMTS, WMS, OGC. BeNomad, Auto CAD (DWG&DXF)
- e) Narzędzie musi umożliwiać stosowanie map od zewnętrznych dostawców takich jak: Google Maps, Bing Maps, ESRI ArcGIS.
- f) Narzędzie musi umożliwiać stosowanie kombinacji map np. map GIS, dostawców internetowych i map własnych użytkownika.
- g) Narzędzie musi pozwalać na tworzenie warstwowej struktury map i wzajemnych połączeń pomiędzy mapami (linków) - nawigowanie pomiędzy mapami musi odbywać się na zasadzie powiększania i pomniejszania np. w skali kraj, miasto, budynek, piętro, pomieszczenie. (bez konieczności korzystania z osobnych drzew nawigacyjnych)
- h) Narzędzie musi posiadać funkcję inteligentnego wyboru obszaru zainteresowania polegającego na możliwości wskazania na mapie obszaru zainteresowania użytkownika, co spowoduje automatyczne wskazanie kamer obserwujących wybrany obszar i ponadto system automatycznie skieruje kamery obrotowe w odpowiednim kierunku, przy uwzględnieniu warunku, że funkcja inteligentnego wyboru musi uwzględnić przeszkody znajdujące się w polu widzenia kamer.

5.3.2. Zaawansowana analityka wideo i mechanizmy inteligencji

- a) Zamawiający wymaga, aby narzędzie Zaawansowanej analityki wideo i mechanizmów inteligencji zostało dostarczone w ramach zadania i pozwalało na uruchomienie narzędzia bez ograniczeń czasowych dla 50 strumieni kamer monitoringu.
- b) Zamawiający wymaga, aby Platforma Bezpieczeństwa posiadała wbudowane mechanizmy obsługi niżej wymienionych funkcjonalności analitycznych i mechanizmów inteligencji:
 - Area protection (obszar chroniony) - wykrywanie ruchu w wyznaczonej strefie w polu widzenia kamery,
 - Perimeter protection (ochrona obwodowa) – wykrywanie wtargnięcia na teren chronionego obiektu z wyznaczonego obszaru
 - Direction of movement (kierunek poruszania się) - wykrywanie kierunku poruszania się osób i pojazdów w polu widzenia kamery,
 - Stopped Vehicle (zatrzymany pojazd) - wykrywanie zatrzymanych pojazdów z powodów niewynikających z warunków ruchu drogowego oraz wykrywanie pojazdów zaparkowanych w miejscach niedozwolonych,
 - Object Detection(detekcja obiektów) - wykrywanie obiektów pozostawionych bez nadzoru np. torby, plecaki, rowery, hulajnogi itp. oraz wykrywanie kradzieży lub dewastacji obiektów małej architektury w przestrzeni publicznej,
 - Tailgating (śledzenie) – wykrywanie wtargnięć do obszarów o ograniczonym dostępie przed wejściem osób niepowołanych za osobą uprawnioną,

5.3.3. Aplikacja Klientka:

- a) Zamawiający wymaga, aby Aplikacja Klientka zapewniała interfejs użytkownika dla konfiguracji i monitorowania w dowolnej sieci, dostępnej lokalnie lub poprzez połączenie zdalne.
- b) Aplikacja Klientka musi być dostępna w co najmniej dwóch językach: polskim oraz angielskim.
- c) Aplikacja Klientka musi posiadać mechanizm autoryzacyjny, który weryfikuje użytkowników.
- d) Zamawiający wymaga, aby logowanie do Aplikacji Klientkiej przebiegało z wykorzystaniem kont i haseł do platformy, przechowywanych lokalnie lub poprzez uwierzytelnienia użytkownika Windows, gdy integracja z Active Directory jest włączona.
- e) Administrator systemu (posiadający wszelkie prawa i przywileje) musi posiadać możliwość definiowania określonych praw dostępu dla każdego użytkownika w systemie (operatora systemu).
- f) Zamawiający wymaga, aby użytkownik systemu mógł uruchamiać wyłącznie określone funkcje systemu oraz realizować konkretne zadania, jeśli posiada do tego przydzielone przez Administratora określone uprawnienia - Platforma Bezpieczeństwa musi posiadać zaimplementowany zespół uprawnień, który będzie umożliwiał nadawanie stosownych uprawnień użytkownikom w celu ukrywania zadań, do których dany użytkownik nie może mieć dostępu.

5.3.4. Pulpit Sterowniczy:

- a) Pulpit Sterowniczy operatora systemu musi posiadać przyjazny i intuicyjny interfejs graficzny, zapewniający użytkownikom kompleksowy widok na kluczowe aspekty działania systemu.
- b) Zamawiający wymaga, aby Pulpit Sterowniczy posiadał funkcję personalizacji, pozwalającej użytkownikom na wybór składowych systemu, które będą wyświetlane na ekranie aplikacji klientkiej oraz ich spersonalizowaną konfigurację.
- c) Administrator systemu musi posiadać możliwość ograniczania użytkownikom zakresu możliwej konfiguracji Pulpitów Sterowniczych poprzez nadawanie stosownych uprawnień.
- d) W ramach Pulpitu Sterowniczego każdy z operatorów systemu musi posiadać możliwość wyboru wyświetlanych na ekranie elementów m.in. takich jak:
 - obraz i kontrola kamer
 - aktywny moduł mapowy
 - raporty
 - zdarzenia i alarmy
 - widżety
 - hiperłącza
 - informacje z systemów zewnętrznych
 - zarządzanie infrastrukturą i użytkownikami
- e) Użytkownik musi mieć możliwość zapisywania swojej konfiguracji Pulpitu Sterowniczego do dalszego wykorzystywania w codziennej pracy. Zapisana konfi-

guracja musi być dostępna dla danego użytkownika z dowolnej stacji roboczej w sieci.

- f) Pulpit Sterowniczy użytkownika musi umożliwiać pracę na tak wielu monitorach, ile akceptuje karta graficzna stacji roboczej oraz system operacyjny z rodziny Microsoft Windows.
- g) Wszystkie informacje wyświetlane na Pulpicie Sterowniczym muszą być odświeżane automatycznie ze zdefiniowaną częstotliwością.

5.3.5. Kliencka Aplikacja Webowa, dostępna przez stronę www:

- a) Zamawiający wymaga, aby w ramach systemu funkcjonowała Kliencka Aplikacja Webowa (klient webowy) dostępna na przeglądarki internetowe takie jak np. Microsoft Internet Explorer, Google Chrome czy Mozilla Firefox.
- b) Jako Kliencką Aplikację Webową należy rozumieć niewielką aplikację niewymagającą instalowania niczego poza przeglądarką internetową.
- c) Strony internetowe klienta webowego muszą być zarządzane i serwowane przez dedykowany do tego celu serwer.
- d) Zamawiający wymaga, aby logowanie do klienta webowego przebiegało z wykorzystaniem kont i haseł do platformy lub poprzez uwierzytelnienia Active Directory.
- e) Połączenie musi być szyfrowane.
- f) Kliencka Aplikacja Webowa działająca w ramach Platformy Bezpieczeństwa musi umożliwiać minimum niżej wymienione funkcje:
 - oglądanie materiału na żywo
 - oglądanie materiału zapisanego
 - sterowanie kamerami PTZ

5.3.6. Aplikacja Mobilna

- a) Zamawiający wymaga, aby w ramach systemu funkcjonowała Aplikacja Mobilna dostępna na urządzenia mobilne tj. smartfony i tablety działające w oparciu o systemy Android oraz iOS.
- b) Aplikacja Mobilna działająca w ramach Platformy Bezpieczeństwa musi umożliwiać minimum niżej wymienione funkcje:
 - oglądanie materiału na żywo
 - oglądanie materiału zapisanego
 - sterowanie kamerami PTZ
 - wykorzystanie kamery urządzenia mobilnego jako kamery systemu VMS

5.3.7. Federacje

- a) Narzędzie Federacji musi umożliwiać tworzenie rozległych, rozproszonych struktur autonomicznych instancji Platformy Bezpieczeństwa wykorzystujących systemy Zarządzania Materiałem Wideo (VMS), Kontroli Dostępu (ACS), czy Automatycznego Rozpoznawania Tablic Rejestracyjnych (ALPR) działającymi w ramach systemów opartych o rozwiązania producenta Platformy Bezpieczeństwa.

- b) Zamawiający wymaga, aby system umożliwiał federowanie zasobów takich jak: kamery monitoringu, kodery wideo, kontrolery drzwi, kart dostępu, alarmy, strefy, jednostki ALPR oraz listy pojazdów.
- c) Narzędzie musi umożliwiać globalne zarządzanie infrastrukturą oraz współdzielenie zasobów, jednocześnie zezwalając na lokalną autonomię systemu podrzędnego z pełną kontrolą nad tym, co jest udostępniane jednostce nadrzędnej.
- d) Narzędzie musi umożliwiać odbieranie zdarzeń w czasie rzeczywistym ze wszystkich zdalnych stron sfederowanych, zarządzanie alarmami, generowanie scentralizowanych raportów, a także kontrolowanie zdalnych kamer PTZ oraz przeglądanie archiwów wideo.
- e) Narzędzie musi zapewniać pełną kompatybilność wstecz i do przodu między federowanymi stronami.
- f) Zamawiający wymaga, aby usługa federacji umożliwiała podłączenie do uruchamianej Platformy Bezpieczeństwa w trybie federacji systemu monitoringu obejmującego Stadion Olimpijski we Wrocławiu działający w oparciu o platformę GSC (Genetec Security Center) i znajdujący się w miejskiej sieci MAN-Wrocław.

5.4. Architektura systemu Zunifikowanej Platformy Bezpieczeństwa:

- 5.4.1. Zamawiający wymaga, aby Zunifikowana Platforma Bezpieczeństwa pracowała w oparciu o architekturę typu klient/serwer tzn. platforma musi składać się z modułu aplikacji serwerowej oraz z aplikacji klienta.
- 5.4.2. Zamawiający wymaga, aby funkcjonowanie Zunifikowanej Platformy Bezpieczeństwa opierało się na architekturze bazującej na rolach. Na każdym serwerze może być uruchomiona jedna lub więcej ról.
- 5.4.3. Komunikacja między serwerem a aplikacją kliencką musi odbywać się w standardzie TCP/IP z możliwością uruchomienia szyfrowania.
- 5.4.4. Serwer Zunifikowanej Platformy Bezpieczeństwa musi pracować jako usługa Windows (uruchamia się wraz ze startem systemu operacyjnego i pracuje w tle).
- 5.4.5. Administrator systemu musi posiadać możliwość uruchomienia platformy na pojedynczym serwerze lub na kilku serwerach o rozproszonej architekturze. Dostarczone rozwiązanie nie może ograniczać liczby uruchomionych serwerów w platformie.
- 5.4.6. Zamawiający wymaga, aby pojedyncza licencja serwerowa Zunifikowanej Platformy Bezpieczeństwa była stosowana na centralnym serwerze odpowiedzialnym za konfigurację i nie było konieczności stosowania odrębnych licencji na żadnej maszynie serwerowej;
- 5.4.7. Dostarczone rozwiązanie musi umożliwiać tworzenie federacji, w której wiele niezależnych instalacji Zunifikowanej Platformy Bezpieczeństwa może być połączone w jeden duży wirtualny system scentralizowanego monitorowania, raportowania i zarządzania alarmami.
- 5.4.8. Zunifikowana Platforma Bezpieczeństwa musi umożliwiać obsługę co najmniej tysiąca aplikacji klienckich podłączonych do systemu jednocześnie. Dowolna liczba aplikacji klienckich może być zainstalowana przez Zamawiającego w dowolnym momencie. Na etapie wdrożenia wymagane jest dostarczenie minimum 30 licencji dla stanowisk operatorskich.

5.4.9. Zunifikowana Platforma Bezpieczeństwa musi umożliwiać rejestrowanie nieograniczonej liczby logów i wpisów historycznych (zdarzenia i alarmy).

5.5. Standardowe role w Zunifikowanej Platformie Bezpieczeństwa:

5.5.1. Zamawiający wymaga, aby system posiadał minimum niżej wymienione role:

- a) rola serwera centralnego
- b) rola rejestratora
- c) rola serwera zarządzającego kamerami wideo
- d) rola monitorowania i raportowania
- e) rola federacji
- f) rola Active Directory
- g) rola zarządzania wtyczkami
- h) rola SDK

5.5.2. Rola serwera centralnego musi realizować minimum takie funkcje jak:

- a) zarządzanie główną bazą danych, zawierającą wszystkie informacje o systemie i konfiguracji komponentów Zunifikowanej Platformy Bezpieczeństwa
- b) autoryzowanie użytkowników i nadawanie dostęp do platformy na podstawie predefiniowanych praw dostępu użytkownika oraz ustawień strefy bezpieczeństwa
- c) konfigurowanie i zarządzanie m.in. następującymi komponentami w podsystemie zarządzania materiałem wizyjnym (VMS):
 - o partycje bezpieczeństwa, użytkownicy i grupy użytkowników;
 - o wejścia/wyjścia (IO);
 - o alarmy;
 - o zdarzenia własne;
 - o makra oraz skrypty własne;
 - o enkodery wideo i ich urządzenia;
 - o sterowanie PTZ;
 - o sekwencje kamer;
 - o harmonogramy nagrywania i archiwizacji;

5.5.3. Rola rejestratora musi realizować minimum takie funkcje jak:

- a) zarządzanie przydzielonymi kamerami i koderami
- b) archiwizowanie wideo

5.5.4. Rola serwera zarządzającego kamerami musi umożliwiać przesyłanie wideo przez sieci lokalne i rozległe (LAN, Internet) ze źródła video (kamera IP, enkoder) do miejsca docelowego (np. aplikacji klienckiej)

5.5.5. Rola monitorowania i raportowania musi realizować minimum takie funkcje jak:

- a) monitorowanie i zapisywanie zdarzeń stanu systemu oraz ostrzeżeń z różnych aplikacji klienta, ról oraz usług, które są częścią platformy
- b) generowanie raportów statystyk dotyczących stanu i historii stanu systemu

- 5.5.6. Rola Federacji musi umożliwiać stworzenie dużego systemu wirtualnego składającego się z nieograniczonej liczby niezależnych i zdalnych systemów Zunifikowanej Platformy Bezpieczeństwa.
- 5.5.7. Rola Active Directory musi umożliwiać synchronizowanie kont użytkowników i kont posiadaczy kart dostępu z serwerem Microsoft Active Directory.
- 5.5.8. Rola zarządzania wtyczkami musi odpowiadać za komunikację pomiędzy Zunifikowaną Platformą Bezpieczeństwa a systemami firm trzecich z których pobierane są niezbędne dane.
- 5.5.9. Rola SDK musi umożliwiać połączenie Zunifikowanej Platformy Bezpieczeństwa z dowolną aplikacją lub interfejsem, który został stworzony z wykorzystaniem SDK.

5.6. Usługa Monitorująca Pracę Serwerów:

- 5.6.1. Zamawiający wymaga, aby Zunifikowana Platforma Bezpieczeństwa posiadała zaimplementowaną usługę Monitorującą Pracę Serwerów (tzw. Watchdog), która nieprzerwanie monitoruje stan usług serwerów.
- 5.6.2. Watchdog musi być realizowany jako usługą Microsoft Windows, która będzie automatycznie uruchamiana podczas startu systemu, niezależnie od tego, czy użytkownik jest zalogowany czy nie.
- 5.6.3. Usługa Monitorująca Pracę Serwerów musi być zainstalowana na wszystkich maszynach serwerowych na których działa serwer Zunifikowanej Platformy Bezpieczeństwa. W wypadku wykrycia błędu lub awarii, Watchdog zrestartuje usługę, w której wystąpił błąd. W ostateczności, Watchdog zrestartuje serwer, jeśli nie będzie w stanie poprawnie uruchomić ponownie usługi.

5.7. Logi:

- 5.7.1. Zunifikowana Platforma Bezpieczeństwa musi umożliwiać tworzenie logów, w których będą znajdować się informacje dotyczące działań operatora/administradora, elementów przez nich dodanych, usuniętych i zmienionych;
- 5.7.2. Logi mogą być generowane jako raporty, które pozwolą na śledzenie zmian dokonanych w określonym czasie (możliwe jest również wyszukiwanie na podstawie określonych użytkowników, zmian, jednostek których dotyczą i przedziałów czasowych);

6. Wymagania techniczne:

6.1. Sprzęt i oprogramowanie:

- 6.1.1. Oprogramowanie musi być zaprojektowane do uruchamiania na typowej platformie PC pracującej pod kontrolą systemu operacyjnego z rodziny Microsoft Windows.
- 6.1.2. Moduł oprogramowania serwerowego musi być kompatybilny z 32 oraz 64 bitowymi wersjami systemów Windows Server 2003 lub nowszymi.
- 6.1.3. Moduł oprogramowania klienckiego musi być kompatybilny z systemami Windows 7 Professional 64-bit PL oraz Windows 10 Professional 64-bit PL.
- 6.1.4. Moduł webowego oprogramowania klienckiego musi być kompatybilny z przeglądarkami internetowymi Internet Explorer, Mozilla Firefox oraz Google Chrome.
- 6.1.5. Moduł mobilnego oprogramowania klienckiego musi być kompatybilny z systemami operacyjnymi Android oraz iOS.

6.2. Kompatybilność względem istniejących rozwiązań serwerowych i macierzowych:

- 6.2.1. Oferowane rozwiązania techniczne muszą być kompatybilne z rozwiązaniami serwerowymi i macierzowymi posiadanymi przez Zamawiającego.
- 6.2.2. Zamawiający dysponuje maszynami klasy HP ProLiant DL360 9-tej generacji z przydzielonymi zasobami ok 40TB na serwer.
- 6.2.3. Zamawiający wymaga utrzymania dotychczasowej retencji materiału wideo z kamer monitoringu na poziomie 30 dni kalendarzowych dla wszystkich kamer włączonych do systemu.

6.3. Kompatybilność względem istniejących stacji roboczych:

6.3.1. Oferowane rozwiązania techniczne oraz licencje muszą być kompatybilne z typowymi stacjami roboczymi, wykorzystywanymi przez Zamawiającego, o niżej wymienionych parametrach:

- procesor: Intel Xeon W-2123 3,60GHz
- pamięć operacyjna: 16 GB ECC
- dysk: 512GB SSD
- procesor graficzny: Nvidia Quadro P2000 5GB GDDR5
- karta sieciowa: 1 GbE
- system operacyjny: Windows 10 Professional 64-bit PL

6.3.2. Jako kompatybilność należy rozumieć możliwość uruchomienia stanowisk operatorskich z wszystkimi wymaganymi funkcjonalnościami systemu przy wyświetlaniu siatek wideo na dwóch ekranach po 12 strumieni z kamer o rozdzielczości FHD 1080p przy bitrate na poziomie 5000kbps z każdej z kamer (łącznie 24 strumienie).

6.4. Kompatybilność względem istniejących kamer:

6.4.1. Oferowane rozwiązania techniczne oraz licencje muszą być kompatybilne z istniejącymi kamerami wykorzystywanymi dotychczas przez Zamawiającego:

- a) Axis Communications M3058-PLVE
- b) Axis Communications P1435-E
- c) Axis Communications P3367-VE
- d) Axis Communications P3717-PLE
- e) Axis Communications P3807-PVE
- f) Axis Communications P5635-E Mk II
- g) Axis Communications Q1786-LE
- h) Axis Communications Q3515-LVE
- i) Axis Communications Q3617-VE
- j) Axis Communications Q3708-PVE
- k) Axis Communications Q6115-E
- l) Axis Communications Q6125-LE
- m) Axis Communications Q6155-E
- n) Bosch VG4-514 analog + VIP-X1 encoder
- o) Bosch VG5-614 analog + VIP-X1 encoder
- p) Bosch VG6-614

- q) Dahua SD6582A-HN
- r) HikVision DS-2DE5220W-AE
- s) HikVision DS-2DF6A236X-AEL
- t) Samsung (Hanwha Techwin) SNO-7084R
- u) Sony SNC-CH120

6.4.2. Jako kompatybilność należy rozumieć możliwość podłączenia istniejących kamer do dostarczanego zunifikowanego systemu bezpieczeństwa w trakcie czynności opisanych w OPZ pkt 3.1.2 ppkt c).

6.4.3. W celu potwierdzenia kompatybilności kamer wskazanych w OPZ pkt 6.4.1 Wykonawca zobowiązany jest złożyć stosowne oświadczenie na etapie składania ofert.

6.5. Kompatybilność względem pulpitów sterowniczych:

6.5.1. Oferowane rozwiązania techniczne oraz licencje muszą być kompatybilne z istniejącymi pulpitemi sterowniczymi wykorzystywanymi dotychczas przez Zamawiającego, tj. umożliwiać podłączenie istniejących paneli sterowniczych USB AXIS T8310 Control Board do stacji roboczych wskazanych w OPZ pkt 6.3.

7. Szkolenia:

7.1.1. Wykonawca zapewni Zamawiającemu szkolenia dla administratorów oraz operatorów systemu.

7.1.2. Szkolenie dla administratorów systemu musi odbyć się na terenie miasta Wrocławia i obejmować przeszkolenie 2 osób wskazanych przez Zamawiającego. W trakcie szkolenia wykonawca zapewni wszelkie niezbędne materiały oraz wyżywienie w przypadku szkolenia całodziennego poza siedzibą Zamawiającego.

7.1.3. Szkolenie dla operatorów musi odbyć się na terenie miasta Wrocławia i obejmować przeszkolenie minimum wszystkich dotychczasowych operatorów systemu Monitoringu Prewencyjnego Wrocławia. Szkolenie operatorów musi odbywać się w formie instruktarzu stanowiskowego, a czas jego trwania nie powinien przekraczać trzech godzin zegarowych.

7.1.4. Preferowanym miejscem przeprowadzenia szkoleń jest siedziba Zamawiającego tj. sala konferencyjna zlokalizowana w budynku Urzędu Miejskiego Wrocławia przy ul. Strzegomskiej 148 we Wrocławiu wyposażona w niezbędny sprzęt audiowizualny, jeżeli Wykonawca uzna, że spełnia ona niezbędne wymagania techniczne i funkcjonalne do przeprowadzenia szkolenia.

7.1.5. Termin przeprowadzenia szkoleń zostanie uzgodniony z Zamawiającym w trybie roboczym w trakcie procesu uruchomienia zintegrowanej platformy bezpieczeństwa.

8. Warunki gwarancji i serwisu:

8.1.1. Gwarancja producenta (SMA - Software Maintenance Agreement) na dostarczane oprogramowanie i licencje (Platformę Bezpieczeństwa) musi wynosić 36 miesięcy.

8.1.2. Zamawiający oczekuje, że serwis gwarancyjny dla zaoferowanej Platformy Bezpieczeństwa będzie umożliwiał obsługę zgłoszeń awarii i zapytań w oparciu o dedykowany serwis www producenta w formie elektronicznej.

8.1.3. Zamawiający otrzyma dostęp do pomocy technicznej www producenta zintegrowanej platformy bezpieczeństwa w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonego oprogramowania

- 8.1.4. Zamawiający wymaga, aby Zunifikowana Platforma Bezpieczeństwa posiadała uruchomiony tryb pracy awaryjnej tzw. "failover" pozwalający na utrzymanie sprawności działania systemu w przypadku wystąpienia awarii poza godzinami pracy serwisu technicznego producenta i zapewnić co do zasady usuwanie awarii w dni robocze, w godzinach pracy Zamawiającego.
- 8.1.5. Wykonawca zapewni wsparcie techniczne dla administratorów systemu w dni robocze w godzinach od 8:00 do 18:00. Wsparcie co do zasady musi odbywać się na zasadach pomocy zdalnej oraz telefonicznej.
- 8.1.6. Wykonawca będzie dokonywać przeglądów serwisowych systemu zgodnie z planem serwisowym wynikającym z zapisów gwarancji producenta systemu, przez cały okres trwania gwarancji, przy czym nie rzadziej niż raz na 12 miesięcy. Wszystkie prace serwisowe w tym zakresie dokonywane będą w siedzibie Zamawiającego.