

ZATWIERDZAM

ZASTĘPCA KOMENDANTA
Centrum Szkolenia Policji w Legionowie

30.04.2023
sierż. Agnieszka ZIELIŃSKA

PROGRAM FUNKCJONALNO – UŻYTKOWY

Nazwa zamówienia:

Wykonanie monitoringu terenu Bazy Szkoleniowej w Kalu

Adres obiektu budowlanego: Baza Szkoleniowa w Kalu
Kal 34
11-600 Węgorzewo

Zamawiający: Centrum Szkolenia Policji w Legionowie
ul. Zegrzyńska 121
05-119 Legionowo

Roboty budowlane

Kod zamówienia według CPV:
51310000-8 – usługi instalowania urządzeń telewizyjnych,
radiowych, dźwiękowych i video,
71220000-6 – usługi projektowania architektonicznego.

Autor opracowania: Piotr Przygoda

CENTRUM SZKOLENIA POLICJI W LEGIONOWIE

kwiecień 2026 rok

NACZELNIK
Wydziału Łączności i Obsługi Informatycznej
Centrum Szkolenia Policji w Legionowie

Jadwiga ŻARNA

NACZELNIK
Wydziału Inwestycji i Remontów
Centrum Szkolenia Policji w Legionowie

Agnieszka CHOJECKA

G-12-5541 DU 9076

C-HF-1844 DU 126

CL-8651 DK 176

Spis treści

Spis treści	3
Część opisowa.....	4
1. Opis ogólny przedmiotu zamówienia.....	4
1.1 Charakterystyczne parametry określające wielkość obiektu lub zakres robót budowlanych.....	4
1.2 Aktualne uwarunkowania wykonania przedmiotu zamówienia	4
1.3 Ogólne właściwości funkcjonalno – użytkowe.....	4
1.4 Szczegółowe właściwości funkcjonalno – użytkowe.....	4
2. Opis wymagań zamawiającego w stosunku do przedmiotu zamówienia.....	4
2.1 Przygotowanie terenu budowy.....	4
2.2 Architektura.....	4
2.3 Konstrukcja.....	4
2.4 Instalacje budowlane.....	5
2.5 Wykończenie.....	5
2.6 Zagospodarowanie terenu.....	5
Część informacyjna.....	5
3.1 Prawo do dysponowania nieruchomością na cele budowlane.....	5
3.2 Gwarancja.....	5
3.3 Informacje ogólne.....	5
3.4 Dokumentacja fotograficzna.....	5

Część opisowa.

1. Opis ogólny przedmiotu zamówienia.

Przedmiotem niniejszego opracowania jest wykonanie monitoringu terenu Bazy Szkoleniowej w Kalu.

1.1 Charakterystyczne parametry określające wielkość obiektu lub zakres robót budowlanych.

Baza Szkoleniowa w Kalu

Powierzchnia działki: 0,34 ha

Powierzchnia użytkowa budynku: 570,62 m²

Kubatura budynku: 3 890 m³

Powierzchnia użytkowa hangaru: 203,40 m²

1.2 Aktualne uwarunkowania wykonania przedmiotu zamówienia

Należy zwrócić szczególną uwagę na prawidłowe zabezpieczenie placu budowy pod kątem porządku oraz bezpieczeństwa użytkowników obiektu.

1.3 Ogólne właściwości funkcjonalno – użytkowe.

W wyniku wykonanych prac wykonany zostanie monitoring terenu Bazy Szkoleniowej w Kalu oraz hangaru.

1.4 Szczegółowe właściwości funkcjonalno – użytkowe.

Nie dotyczy.

2. Opis wymagań zamawiającego w stosunku do przedmiotu zamówienia.

2.1 Przygotowanie terenu budowy.

Nie dotyczy.

2.2 Architektura.

Nie dotyczy.

2.3 Konstrukcja.

Nie dotyczy.

2.4 Instalacje budowlane.

Wykonanie monitoringu terenu Bazy Szkoleniowej w Kalu i hangaru należy wykonać zgodnie z założeniami zawartymi w załączniku nr 1.

2.5 Wykończenie.

Nie dotyczy.

2.6 Zagospodarowanie terenu.

Nie dotyczy.

Część informacyjna.

3.1 Prawo do dysponowania nieruchomością na cele budowlane.

Zamawiający oświadcza, że posiada prawo do dysponowania nieruchomością na cele budowlane.

3.2 Gwarancja.

Wymagany minimalny okres gwarancji na urządzenia: 2 lata.

Okres gwarancji będzie liczony od daty odbioru końcowego.

3.3 Informacje ogólne.

Zamawiający zaleca dokonanie wizji lokalnej obiektu. Termin należy uzgodnić z przedstawicielem Wydziału Administracyjno-Gospodarczego Centrum Szkolenia Policji w Legionowie.

Wykonawca zobowiązany jest do uzgadniania na bieżąco z Zamawiającym urządzeń przewidzianych do montażu oraz poszczególnych etapów prac.

Po wykonaniu prac wykonawca sporządzi dokumentację techniczną powykonawczą.

Prace branży teletechnicznej muszą być wykonane przez osobę (1 osoba) posiadającą uprawnienia SEP „E” do 1kV.

Prace związane z monitoringiem muszą być wykonane przez pracownika wpisanego na listę pracowników zabezpieczenia technicznego (1 osoba).

3.4 Dokumentacja fotograficzna

Dokumentacja fotograficzna w załączniku nr 2.

Założenia do wykonania monitoringu na terenie Bazy Szkoleniowej w Kalu oraz w hangarze

Założenia projektu

Na terenie Bazy Szkoleniowej w Kalu należy zaprojektować serwer nagrywający który będzie obsługiwał do 100 kamer/końcówek w rozdzielczości 4K z archiwum 30 dniowym. Ponadto należy przewidzieć, że dla wyżej wymienionego serwera nagrywającego należy zaprojektować zapasowy serwer nagrywający. Który przejmie rolę w momencie jakiegokolwiek awarii i zachowa ciągłość archiwum. Serwer zapasowy ma przechowywać archiwum przez 14 dni.

Sposób licencjonowania musi się odbywać w sposób przejrzysty per kamera/końcówka. Ilość licencji można dowolnie zwiększać poprzez dokupienie kolejnych. Licencja musi być wieczysta. Licencje muszą posiadać dwuletni dostęp do aktualizacji oprogramowania. Po wygaśnięciu oprogramowania ma nadal działać. Ponadto musi być zapewnione wydłużenie wsparcia na dostęp do aktualizacji do pięciu lat lub dożywotnio.

Oprogramowanie nie może być ograniczone górną ilością lokalizacji dodanych do systemu ani ilością użytkowników korzystających jednocześnie z systemu.

Zamawiający zapewni połączenie lokalizacja <-> centrala jest wymagana do wymiany plików konfiguracyjnych. Strumienie z kamer obsługiwane będą w ramach lokalizacji, nie jest wymagane przesyłanie strumieni do centrali w sposób ciągły.

System musi mieć możliwość ustanowienia lokalnego administratora systemu, który będzie miał dostęp do elementów tylko ze swojego zakresu.

Wykonanie monitoringu – wymagania

Przedmiotem zamówienia jest kompleksowe dostarczenie systemu wideo monitoringu. W którego skład wchodzi: kamery wraz z montażem oraz okablowaniem, system zarządzający wraz z osprzętem (w tym serwery z dyskami oraz stacja robocza z monitorem dla użytkownika).

Zadanie obejmuje kompleksowe wykonanie monitoringu ochrony terenu ośrodka, wnętrza budynku, pomostu oraz rejestrację samochodów wjeżdżających oraz wyjeżdżających z terenu Bazy Szkoleniowej w Kalu.

System musi umożliwiać lokalny zapis obrazu z każdej z kamer w ich natywnej rozdzielczości 24/7, a także możliwość podglądu obrazu z danej kamery w czasie rzeczywistym.

Lokalna konfiguracja urządzeń i Systemu Zarządzania Sygnałem Wizyjnym (Video Management System – VMS) musi być przygotowana na integrację z kamerami analitycznymi.

Wszystkie urządzenia Systemu Monitoringu Wizyjnego muszą być fabrycznie nowe. Urządzenia muszą posiadać oznaczenie CE.

System Monitoringu Wizyjnego musi zapewniać szczegółowość odwzorowania odpowiadającą rozpoznawaniu, obserwowaniu, identyfikowaniu bądź inspekcjonowaniu zależnie od zakresu obiektu. Urządzenia do rejestracji materiału wideo z System Monitoringu Wizyjnego muszą spełniać warunki techniczne jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Zapisywany obraz powinien być uzupełniony stemplem czasowym o rozdzielczości 1 s. W celu eliminowania błędu stempla czasu, data i czas urządzenia rejestrującego muszą być synchronizowane z serwerami czasu.

Wymagania techniczne:

Wymagania ogólnofunkcjonalne dla systemu zarządzania video (VMS)

Parametry minimalne i wymagania funkcjonalne dla systemu zarządzania bezpieczeństwem – licencja dla Etapu 1 i 2. Lokalizacja KAL przewiduje 50 licencji / końcówek z możliwością zwiększenia do 100 licencji:

Oferowany system musi spajać w sposób logiczny i przez wspólny interfejs użytkownika co najmniej 4 własne moduły: zarządzanie źródłami video, kontrola dostępu, rozpoznawanie tablic rejestracyjnych, rozpoznawanie twarzy.

Oferowany system musi być otwarty, z ogólnodostępnym Software Development Kit (SDK). Funkcjonalność ta powinna umożliwiać w razie potrzeby integrację z dowolnymi kamerami CCTV IP, zewnętrznymi systemami alarmowymi i kontroli dostępu.

System musi oferować możliwość integracji wykorzystując protokół OPC. Dopuszcza się stosowanie zewnętrznych modułów integracji OPC, o ile są. Jeśli funkcjonalność wymaga dodatkowej licencji powinna być ona dostarczona wraz z systemem.

System musi oferować możliwość integracji wykorzystując protokół MODBUS. Dopuszcza się stosowanie zewnętrznych modułów integracji MODBUS, o ile są. Jeśli funkcjonalność wymaga dodatkowej licencji powinna być ona dostarczona wraz z systemem.

System musi oferować możliwość integracji wykorzystując protokół MQTT. Dopuszcza się stosowanie zewnętrznych modułów integracji MQTT, o ile są. Jeśli funkcjonalność wymaga dodatkowej licencji powinna być ona dostarczona wraz z systemem.

System musi oferować możliwość integracji z usługą Active Guard. Dopuszcza się stosowanie zewnętrznych modułów integracji Active Guard, o ile są. Jeśli funkcjonalność wymaga dodatkowej licencji powinna być ona dostarczona wraz z systemem.

Otwartość systemu musi umożliwiać wykorzystanie będących w powszechnej dystrybucji stacji klienckich, serwerów urządzeń infrastruktury sieci oraz pamięci masowych.

System musi posiadać możliwość dekodowania strumieni H.264 oraz H.265 po stronie karty graficznej, z możliwością przydzielenia dedykowanych kart do poszczególnych kodeków.

System musi obsługiwać kodeki MJPEG, MPEG4, H.264, H.265, MxPEG

System musi być oprogramowaniem pracującym w architekturze klient-serwer. Część serwerowa musi odpowiadać za wszystkie procesy związane z rejestracją i zarządzaniem oraz udostępnianiem danych do stacji klienckich, natomiast część kliencka ma odpowiadać jedynie za pobieranie i wizualizowanie tych danych. Serwer platformy może zostać uruchomiony na pojedynczym serwerze lub na kilku serwerach w rozproszonej

architekturze. Cała komunikacja między serwerem a aplikacją kliencką oparta jest na standardowym protokole TCP/IP wraz z możliwością uruchomienia szyfrowania.

VMS musi zapewniać elastyczność i możliwość integracji, dlatego musi obsługiwać wideo dekodery (wideoserwery przetwarzające analogowe sygnały wideo na strumienie cyfrowe) oraz kamery IP, różnych producentów, w tym: AXIS, ACTI, ARECONT, AVIGILON, AIRLIVE, AVER, AVTECH, BASLER, CANON, D-LINK, DAHUA, DYNACOLOR, ENEO, i-PRO, FLIR, GANZ, FOSCAM, GEOVISION, HANWHA, HIKVISION, HUNT, IQEYE, JVC, LEICA, LG, LEVELONE, MOBOTIX, MILESIGHT, MOXA DECODERS, MOXA I/O, PELCO, PANASONIC, SAMSUNG, SONY, SUNELL, TOA, TVT, UNIVIEW, UTC, VIVOTEC, YUDOR, ZAVIO, Y-CAM, ZENITEL. System musi umożliwiać podgląd jak i rejestracje urządzeń podłączonych po USB (kamery inspekcyjne, kamery web, skanery, kamery termowizyjne itp.) bez limitu kanałów.

Oprogramowanie musi w sposób wizualny informować operatora o typie urządzenia dodanego do systemu (kamera typu tuba, kopułka, szybkoobrotowa, strona internetowa, smartfon, głośnik, itp.).

Oprogramowanie musi posiadać funkcjonalność, pozwalającą na sterowanie kamerą szybkoobrotową poprzez kliknięcie w interesujący obszar na scenie.

System VMS w celu zapewnienia elastyczności musi umożliwić natywną integrację z popularnymi systemami kontroli dostępu, w tym przynajmniej z Roger RACS 5, Gallagher Command Centre, Iron Wave, Paxton, NEDAP, Kantech, Satel Integra. Integracja musi umożliwiać wyszukiwanie nagrań wykorzystując dane zapisane po stronie kontrolera kontroli dostępu. System musi umożliwić tworzenie wewnętrznych i zewnętrznych zdarzeń (automatyczne zakładki wideo, pop-up, email, żądania HTTP, wyzwalanie wyjść alarmowych, zmiana stanu strefy z wizualizacją na mapie, presetów itp.) na podstawie zdarzeń z kontroli dostępu. Jeśli taka funkcjonalność wymaga dodatkowej licencji, powinna być ona dostarczona wraz z systemem. W celu scentralizowania i usprawnienia pracy systemu, VMS musi umożliwiać natywną integrację z popularnymi systemami alarmowymi, w tym przynajmniej z SATEL INTEGRA. Jeśli taka funkcjonalność wymaga dodatkowej licencji, powinna być ona dostarczona wraz z systemem. Bez limitu ilości elementów kontroli dostępu oraz systemu alarmowego.

System VMS musi umożliwiać wsparcie dla kamer obsługujących ONVIF. Integracja ONVIF musi umożliwiać obsługę detekcji ruchu, strumienia audio, wejść/wyjść alarmowych, analizy obrazu, zapisu i synchronizacji nagrań z kart pamięci (tak zwane EDGE recording lub ANR – Automatic Network Replenishment) jeśli kamera jest zgodna z odpowiednim profilem ONVIF

Aplikacja serwerowa systemu musi posiadać wbudowany silnik analizy obrazu, bazujący na sieciach neuronowych i umożliwiać uruchomienie takiej analizy obrazu na dowolnym strumieniu wideo (RTSP, MJPEG, MxPEG, ONVIF) jak również do już zarejestrowanego materiału (pliki AVI). Analiza obrazu powinna umożliwiać filtrowanie zdarzeń na podstawie wykrytych obiektów, lista powinna zawierać przynajmniej następujące obiekty: samochód osobowy, bus, ciężarówka, łódź, człowiek, motocykl, rower, zwierzę. Licencja za analizę obrazu nie powinna być przypisana na stałe dla danego kanału,

powinna umożliwiać dowolne przenoszenie w ramach strumieni wideo dostępnych w systemie.

System musi posiadać możliwość zliczania dowolnych zdarzeń z analizy obrazu, wejść alarmowych i czujników zewnętrznych. Zliczanie powinno odbywać się na dowolnej liczbie kamer i urządzeń z możliwością sumowania i odejmowania. System musi umożliwiać tworzenie zdarzeń i procedur na podstawie wartości poszczególnych liczników. Dodatkowo system musi umożliwiać tworzenie raportów na podstawie zliczonych zdarzeń.

Oprogramowanie musi umożliwiać wykorzystanie brzegowej analizy obrazu (np. odczyt tablicy rejestracyjnej) i umożliwiać reakcję na zdarzenia wygenerowane przez analizę obrazu (automatyczne zakładki wideo, pop-up, email, żądania HTTP, wyzwalamie wyjść alarmowych, zmiana stanu strefy z wizualizacją na mapie, presetów itp.)

System musi umożliwiać tworzenie automatycznych zakładek na materiale wideo. Zakładki powinny być tworzone automatycznie, wraz z automatycznym opisem (rodzaj zdarzenia, numer zdarzenia, kamera, lokalizacja) jako wynik analizy obrazu (zarówno na kamerze jak i po stronie serwera), detekcji ruchu, wartości licznika, zdarzeń systemowych, danych POS, komend CGI i żądań http z aplikacji zewnętrznych (wymagane w celach integracji i aby zapewnić elastyczność systemu). W zakładkach musi być możliwość umieszczania komentarzy z informacją, który użytkownik systemu taki komentarz dodał. Jeśli funkcjonalność tworzenia zakładek wymaga dodatkowej licencji, musi być ona dostarczona wraz z systemem.

System musi umożliwiać rejestrowanie strumieni wideo wysyłanych na żywo z urządzeń Android i iOS wraz z ich położeniem przesłanym na podstawie GPS. Dopuszcza się stosowanie dedykowanej aplikacji po stronie urządzenia do wysyłania obrazu. Funkcjonalność powinna być zintegrowana i dostarczona wraz z aplikacją serwerową i powinna być dostępna dla wszystkich kanałów dostępnych dla danej licencji.

System musi wspierać koncepcję federacji, czyli wiele niezależnych instalacji VMS może być połączonych w jeden duży wirtualny system scentralizowanego monitorowania, raportowania i zarządzania alarmami jak również zarządzania użytkownikami (tworzenie, przydzielanie ról i uprawnień, oraz monitoring zajętości pasma sieciowego i zasobów serwera).

System VMS i jego komponenty (aplikacja serwerowa, konsola, aplikacja kliencka) musi posiadać możliwość pracy w środowisku wirtualnym. Jeśli taka funkcjonalność wymaga dodatkowej licencji, powinna być ona dostarczona wraz z systemem.

System VMS i jego komponenty (aplikacja serwerowa, konsola, aplikacja kliencka) musi być dostępna w wersji 32 oraz 64 bitowej. Jeśli taka funkcjonalność wymaga dodatkowej licencji, powinna być ona dostarczona wraz z systemem.

System VMS musi umożliwiać tworzenie interaktywnych przycisków umożliwiających wywoływanie komend CGI, wysyłanie żądań http, resetowanie liczników, generowanie alarmów, uzbrajanie/rozbrajanie systemów alarmowych, wyzwalamie wyjść alarmowych. System musi również umożliwiać inne działanie dane przycisku w zależności od zmiennych przydzielanych przez system (np. inne działanie przycisku w zależności poziomu temperatury podanym przez czujnik temperatury w serwerowni). System VMS

musi umożliwiać stworzenie dowolnej ilości przycisków bez wymogu dodatkowych licencji.

Licencja na system VMS nie powinna być przypisana do specyfikacji sprzętowej serwera i umożliwiać przenoszenie na inne serwery bez ingerencji producenta.

System musi umożliwiać połączenie 250 klientów (android, iOS, aplikacja kliencka, przeglądarka) w tym samym momencie. Jeśli taka funkcjonalność wymaga dodatkowej licencji, powinna być ona dostarczona wraz z systemem.

System VMS musi posiadać funkcję audytu, która będzie rejestrowała w osobnej, szyfrowanej bazie danych, wszystkie zdarzenia i akcje podejmowane przez dowolnego użytkownika na stacji klienckiej jak i aplikacji serwerowej.

Aby zapewnić łatwość integracji z zewnętrznymi systemami i czujnikami, system musi posiadać wbudowany tak zwany sniffer danych wysyłanych na port COM, wybrany port sieciowy oraz API. Sniffer musi umożliwiać filtrowanie przesyłanych danych w celu wyodrębnienia ciągów znaków i używania ich jak zmiennych w systemie (dane liczbowe, np. z czujników, wag drogowych) jak również opisów do automatycznych zakładek. System musi umożliwiać tworzenie zdarzeń (wysyłanie email, okna pop-up, notyfikacje push) na podstawie zdefiniowanych ciągów znaków. Jeśli ta funkcjonalność wymaga dodatkowej licencji, powinna być ona dostarczona wraz z systemem.

VMS będzie działał na standardowych systemach operacyjnych Windows i różnych mobilnych systemach operacyjnych dla platform opartych na aplikacjach mobilnych.

VMS musi obsługiwać funkcję multicastu, a także możliwość unicastu dla każdego urządzenia peryferyjnego kamery w wielu instancjach jednocześnie.

Producent systemu VMS musi umożliwiać świadczenie wsparcia (aktualizacji, poprawek) dla systemu na okres 2 lat z możliwością rozszerzenia do 5 lat lub dożywotniego zgodnie z polityką Producenta systemu. Wsparcie Producenta oraz Oferenta musi wynosić min 2 lata.

Federacja: Obsługa zdalnych systemów:

Funkcja federacji zezwala na połączenie wielu niezależnych systemów VMS (systemów sfederowanych) w większy system wirtualny (Federację). Umożliwia to globalne monitorowanie wielu niezależnych systemów VMS producenta.

VMS musi działać w architekturze federacyjnej umożliwiającej każdemu upoważnionemu użytkownikowi bezproblemowy dostęp do zasobów systemowych (takich jak wideo na żywo/nagrane) podłączonych do dowolnego serwera sieciowego.

Architektura federacyjna umożliwi również scentralizowaną administrację serwerów aplikacji, aplikacji klienckich i koderów/aparatów cyfrowych w celu aktualizacji oprogramowania, oprogramowania układowego, dystrybucji alarmów i alertów oraz tworzenia kopii zapasowych danych konfiguracyjnych.

Funkcja federacji musi unifikować wiele odrębnych (logicznie, lub geograficznie) systemów bezpieczeństwa.

Federacja musi obsługiwać alarmy i kamery.

System musi umożliwiać nagrywanie dowolnego ekranów innych stacji klienckich i serwerów wraz z obsługą nagrywania ściany wizyjnej.

Integracja z Microsoft Active Directory – możliwość:

Platforma VMS pozwala na bezpośrednie połączenie z jednym lub wieloma serwerami Microsoft Active Directory poprzez Role AD. Integracja z Active Directory umożliwia synchronizację informacji serwera Active Directory.

Jeśli zezwolono, Active Directory zarządza logowaniem użytkowników do aplikacji klienckiej platformy VMS poprzez poświadczenia użytkownika Windows. Logowanie do platformy VMS wykorzystuje opcje zarządzania hasłami i autoryzacji Active Directory. Dodawanie, usuwanie lub zawieszanie konta użytkownika Windows w Active Directory skutkuje utworzeniem, usunięciem lub wyłączeniem odpowiedniego konta użytkownika w platformie VMSX

Praca awaryjna (Failover), czuwanie (Standby), bezpieczeństwo:

System musi obsługiwać własne opcje pracy w przypadku wystąpienia awarii (failover).

System musi umożliwiać obsługę serwerów centralnych (standby) działający jako serwery zastępcze pracujące w trybie czuwania. W przypadku awarii dowolnego serwera w systemie, serwer centralny przejmie wszystkie połączenia oraz ustawienia takiego serwera. Przejęcie może nastąpić w czasie krótszym niż 2 minuty. Nie powinno to wymagać ingerencji użytkownika. System powinien umożliwiać konfigurację czasu po jakim serwer standby określa awarię serwera VMS. System musi umożliwiać redundancję „n do 1”, jak również „1 do n”. System musi umożliwiać stworzenie minimum 4 serwerów redundantnych. Przejęcie przez serwer standby musi odbywać się kaskadowo. Jeśli taka funkcjonalność wymaga dodatkowej licencji, powinna być ona dostarczona wraz z systemem.

Zapasowy serwer centralny powinien mieć możliwość zachowania bazy danych konfiguracji zsynchronizowanej z głównym serwerem centralnym.

System VMS musi umożliwiać tworzenie oddzielnych baz danych dla zdarzeń, użytkowników, nagrań oraz dla audytu systemu wraz z oddzielnym sposobem szyfrowania.

System musi automatycznie szyfrować wszystkie bazy danych (również bazę nagrań), jak również dodatkowo zabezpieczać je hasłem.

System musi wykorzystywać tunelowanie HTTPS SSL/TLS, w celu zabezpieczania komunikacji serwer-serwer, serwer-klient, serwer-kamera nie tylko przy użyciu hasła, ale również szyfrowania całej transmisji (zabezpieczanie nie tylko komunikatu, ale również komunikacji, aby zminimalizować ryzyko ataku man-in-the-middle)

VMS musi wykorzystywać czasowe tokeny do zestawiania połączeń sieciowych, aby zabezpieczyć system przed atakami DoS.

System musi umożliwiać tworzenie własnych polityk haseł użytkowników, definiujących długość hasła, ilość prób logowania, ilość znaków specjalnych.

System musi umożliwiać definiowanie co do minuty długości archiwum do jakiego dostęp ma dany użytkownik, bez względu na to jak długie archiwum znajduje się na serwerze.

System musi dokumentować wszystkie zmiany związane z użytkownikiem w aplikacji i podłączonych urządzeniach peryferyjnych ze środowiskiem aplikacji.

Aplikacja Klientka:

Aplikacja kliencka musi zapewnić interfejs użytkownika dla konfiguracji i monitorowania w dowolnej sieci, dostępnej lokalnie lub poprzez połączenie zdalne.

Wszystkie aplikacje muszą posiadać mechanizm autoryzacyjny, który weryfikuje użytkownika. Dzięki temu administrator (posiadający wszelkie prawa i przywileje) może zdefiniować określone prawa dostępu dla każdego użytkownika w systemie.

Logowanie do aplikacji klienta musi przebiegać poprzez konta i hasła systemu przechowywane lokalnie lub poprzez uwierzytelnienia użytkownika Windows, gdy integracja z Active Directory jest włączona.

Aplikacja kliencka musi być dostępna w języku polskim.

Aplikacja kliencka musi mieć możliwość zablokowania powłoki Windows, aby uniemożliwić zamknięcie czy zminimalizowanie aplikacji bez podania hasła nadanego przez administratora.

Aplikacja kliencka musi posiadać interfejs do wygodnego przeglądania nagrań ze wszystkich wyświetlonych kamer (od 1 do 100 jednocześnie). Interfejs powinien posiadać oś czasu obrazującą obecność nagrań, jak również zaznaczone okresy detekcji ruchu (oddzielne kolory dla detekcji po stronie serwera jak i po stronie kamery), nagrywania ciągłego, nagrywania po zdarzeniu z analizy obrazu (zarówno z kamery jak i z serwera).

Aplikacja kliencka musi posiadać interfejs do eksportowania nagrań z min. 72 kamer jednocześnie. Użytkownik powinien mieć możliwość eksportu nagrań z wielu kamer w postaci pojedynczych plików, jak również w postaci jednego pliku mozaikowego złożonego z nagrań wszystkich wyświetlonych kamer (wsparcie dla rozdzielczości 8K dla pliku wyjściowego).

Aplikacja kliencka musi mieć możliwość odtwarzania materiały z przyspieszeniem 128x oraz spowolnieniem 128x.

System będzie w stanie pobierać nagrane wideo na podstawie kryteriów wyszukiwania użytkowników, w tym kombinacji:

- identyfikator referencyjny kamery,
- data i godzina nagrania z kamery,
- zaznaczenie obszaru wokół interesującego obiektu w celu ustalenia, kiedy obiekt pojawił się w scenie,
- zdarzenia alarmowe,
- zakładki dodawane automatycznie lub ręcznie przez użytkownika,
- alfanumeryczny ciąg metadanych (np. numer transakcji nagrany za pomocą wideo z innych systemów, numery tablic rejestracyjnych, kody kreskowe, dane z wag itp.).

VMS zbuduje pojedynczy, złożony plik do eksportu zawierający sekwencję wybranych nagrań z kamer, w których materiał musi być zbudowany z wielu sekwencji, kamer i pól widzenia w czasie.

VMS musi posiadać funkcjonalność rozmywania ruchu na eksportowanym materiale wideo. Jeśli funkcjonalność wymaga dodatkowej licencji powinna być ona dostarczona wraz z systemem.

Aplikacja musi oferować interfejs do wyszukiwania ciągów znaków odbieranych i filtrowanych przez sniffer po stronie serwera.

Aplikacja musi oferować podłączenie i wyświetlanie strumieni wideo na co najmniej 10 monitorach. Jeśli funkcjonalność wymaga dodatkowej licencji powinna być ona dostarczona wraz z systemem.

Tam, gdzie pozwalają na to zasady i przepisy, system będzie miał możliwość integracji 1- lub 2-stronnej komunikacji głosowej w celu obsługi funkcji wideo w różnych lokalizacjach w zależności od potrzeb użytkownika.

Mapy:

System musi posiadać zintegrowane narzędzie do edycji i tworzenia map rozmieszczenia elementów technicznego systemu zabezpieczeń. Graficzny interfejs mapy musi spełniać co najmniej następujące wymagania:

- wyświetlanie wielu map dla jednego oraz dla wielu obszarów,
- wyświetlanie map jako warstw,
- wyświetlanie podkładów mapowych w postaci map GIS np. OpenStreetMap, Google Map, TomTom. Jeśli funkcjonalność wymaga licencji musi być ona dostarczona wraz z systemem, dla minimum 10 map GIS,
- wyświetlanie podkładów mapowych w postaci bitmap,
- przełączanie się pomiędzy mapami poprzez aktywne przyciski, również między mapami GIS i bitmapami,
- wyświetlanie na mapie aktywnych ikon urządzeń w systemie,
- wyświetlanie na mapie aktywnych obszarów obserwacji kamer stacjonarnych w systemie,
- wyświetlanie na mapie aktywnych ikon urządzeń powiązanych z alarmami takich jak status drzwi z kontroli dostępu, czujki ruchu, bariery podczerwieni. Wraz z możliwością definiowania własnych ikon i ich kolorów i stanów.

Centralne zarządzanie mapami.

Otwarta architektura:

System musi być neutralny w stosunku do producentów urządzeń technicznych systemów bezpieczeństwa dostępnych na rynku i umożliwiać ich integrację udostępniając Software Development Kits (SDK), Driver Development Kits (DDK), Web Service SDK.

System musi posiadać możliwość dodania plug-inów integrujących systemy zewnętrzne, takie jak:

- analityka wideo
- zewnętrzne systemy firm trzecich

Wszystkie kamery podłączone do VMS muszą być sterowane przez dowolne urządzenie wejściowe. Obejmuje to między innymi mysz, joysticki, panele sterowania, ekran dotykowy, urządzenia podłączone poprzez Bluetooth, urządzenia mobilne lub urządzenia wejściowe z klawiaturą.

Dodatkowe funkcje systemu:

System musi umożliwiać tworzenie i zarządzanie ścianą wideo, poprzez zastosowania stacji komputerowych typu desktop i dołączonych monitorów, zamiast dedykowanego rozwiązania dla ścian wideo. System musi umożliwiać stworzenie minimum 10 niezależnych ścian wizyjnych. Każda ze ścian wizyjnych musi obsługiwać minimum 9 monitorów. Jeśli funkcjonalność wymaga dodatkowej licencji powinna być ona dostarczona wraz z systemem.

Architektura platformy VMS powinna umożliwiać pełną skalowalność i ma umożliwiać rozbudowę systemu, zależnie od potrzeb o:

- co najmniej 1 000 serwerów rejestracji i zarządzania
- co najmniej 500 stacji klienckich
- co najmniej 15 000 kamer
- co najmniej 15 000 modułów wejść/wyjść alarmowych

System musi posiadać usługę nieprzerwanie monitorującą pracę i stan usług serwerów. Usługa monitorująca musi działać w środowisku Windows i być automatycznie uruchamiana podczas startu systemu niezależnie od tego czy użytkownik jest zalogowany czy nie.

W wypadku wystąpienia błędu lub awarii usługa monitorująca musi restartować usługę w której wystąpił błąd, a w ostateczności uruchomić ponownie serwer/komputer jeśli nie jest w stanie uruchomić ponownie usługi.

Usługa powinna zapisywać zdarzenia w wydzielonej, szyfrowanej i zabezpieczonej hasłem bazie danych.

System musi posiadać ramy usług konserwacji i naprawy wsparcia, aby zapewnić integralność systemu, bezpieczeństwo i ciągłość działania.

System musi posiadać moduł samo oceniający cyber bezpieczeństwo systemu wraz z instrukcjami jak podnieść poziom bezpieczeństwa,

Usługi dodatkowe:

Możliwość wykupienia wsparcia Producenta do 11 lat od chwili zakupu

W oferowanym rozwiązaniu musi zostać wliczone 2 letnie wsparcie Producenta systemu oraz Oferenta

W ofertę musi być wliczona dostawa, instalacja oraz szkolenie z obsługi.

Inne:

Wymaga się aby system VMS wdrażała firma posiadająca aktualny certyfikat producenta sprzętu z zakresu instalacji oraz uruchomienia. Zapewni to lepszą jakość wykonanej pracy oraz umożliwi ewentualne wsparcie producenckie na etapie uruchamiania systemu oraz szkolenia personelu z obsługi systemu.

Zaleca się aby Wykonawca przedstawił referencję z wdrożenia podobnych systemów.

System powinien umożliwić obsługę min. 600 szt. kamer. Czas zapisu zależnie od lokalizacji.

Wymaga się aby wszystkie elementy systemu system były zgodne z ustawą NDAA, TAA oraz spełniały zalecenia dyrektywy NIS2.

Wymaga się aby zintegrować z systemem istniejące kamery IP.

Serwer – 2 szt.

Serwer GIGUS 3U16B-1700	
Procesor	Procesor powinien posiadać nie mniej niż 9 rdzeni i 15 wątków, Taktowanie zegara nie niższe niż 3,60 GHz, Wynik całosciowy w passmark nie mniejszy niż 27200 pkt, Wynik rdzenia w passmark nie mniejszy niż 3900 pkt, Pamięć Cache poziomu trzeciego nie mniejsza niż 19 MB, Pobór prądu nie wyższy niż 165 W, Dołączony wydajny układ chłodzenia, Zintegrowany układ graficzny.
RAM	Pamięć RAM nie mniejsza niż 32 GB, Taktowanie pamięci nie mniejsze niż 4800 MHz, Pamięć powinna być nie starsza niż 5 generacji.
Płyta główna	Płyta główna powinna umożliwiać obsługę pamięci RAM co najmniej 128 GB, w standardzie DDR5-4400 MHz, Płyta główna musi być kompatybilna z oferowanym procesorem i umożliwiać kompatybilność z innymi procesorami. Płyta główna powinna posiadać co najmniej 4 gniazda DIMM, Płyta główna powinna posiadać co najmniej 2 gniazda PCI-E 5.0 x16, Płyta główna powinna posiadać co najmniej 2 gniazda PCI-E 3.0 x4, Płyta główna powinna posiadać co najmniej 1 gniazdo PCI 32 bit, Płyta główna powinna posiadać co najmniej 3 złącza M.2 z możliwością konfiguracji RAID 0 i 1, Płyta główna powinna posiadać co najmniej 8 złącz SATA3 z obsługą RAID 0,1,5,10, Płyta główna powinna posiadać co najmniej 3 złącza Ethernet, Płyta główna powinna posiadać co najmniej 2 złącza cyfrowe video.
Dyski twarde/ dyski półprzewodnikowe	Serwer powinien być wyposażony w 2 dyski SSD NVMe o pojemności min. 500 GB, które powinny być skonfigurowane w RAID 1, by uchronić przed uszkodzeniem. Prędkość odczytu/zapisu dysku powinna być nie mniejsza niż 4000 MB/s.
Interfejsy sieciowe	Serwer powinien posiadać co najmniej 1 interfejs sieciowy o przepustowości 2,5 Gbps, Serwer powinien posiadać co najmniej 1 interfejs sieciowy o przepustowości 1 Gbps, Serwer powinien posiadać sieciowy interfejs konsolowy. Serwer powinien umożliwiać montaż i obsługę dodatkowej kart sieciowych LAN/SFP.
Karty rozszerzeń	Serwer powinien być wyposażony w kontroler RAID obsługujący 16 dysków, wielkość pamięci podręcznej cache nie mniejsza niż 1GB, z możliwością konfiguracji RAID 0,1,10,5,6,50,60. Do kontrolera powinno zostać dostarczone niezbędne okablowanie.

GPU	Serwer powinien posiadać zintegrowany układ graficzny, umożliwiający wyświetlanie obrazu na monitorze. Serwer powinien umożliwiać montaż i obsługę dodatkowej karty graficznej z rdzeniami CUDA.
System operacyjny	Serwer musi być kompatybilny i umożliwiać instalację z systemami Windows oraz Linux.
Obudowa	Serwer musi posiadać obudowę typu RACK, Serwer powinien posiadać co najmniej 16 zatok dyskowych 3,5", Serwer powinien posiadać wbudowany zasilacz, Do serwera powinny być dołączone akcesoria montażowe do szaf typu RACK.
Zasilanie	Serwer powinien posiadać 2 zasilacze umożliwiające redundancję zasilania, Moc zasilacza powinna zostać wyliczona pod zaproponowane komponenty z uwzględnieniem 20% zapasu mocy. Zasilacz musi posiadać co najmniej 80% sprawność elektryczną.
Gwarancja	Serwer powinien posiadać gwarancję minimum 2 lata, typu Next Business Day (NBD). Możliwość wydłużenia gwarancji do 60 miesięcy.

Dyski do serwera – 6 szt.

Dysk twardy HDD 3,5"	
Typ	Dysk twardy do pracy ciągłej klasy Enterprise
Rozmiar fizyczny	3,5"
Pojemność	Nie mniejsza niż 22 TB (22 000 GB)
Prędkość talerza	Prędkość obracania talerza nie mniejsza niż 7200 obr./min
Rodzaj gazu wypełniającego	Dysk twardy musi być wypełniony helem.
Wielkość bloków	Dysk twardy musi posiadać blok nie mniejszy niż 512e B.
Wielkość buforu	Dysk twardy musi posiadać bufor nie mniejszy niż 512 MiB.
Szybkość przesyłania danych	Dysk twardy musi pozwalać na przesyłanie danych ze stałą prędkością nie mniejszą niż 284 MB/s.
Pobór prądu	Dysk twardy musi pobierać nie więcej niż 10,5 W.
Żywotność	Średni czas wystąpienia awarii musi być nie mniejszy niż 2,5 mln godzin.
Wskaźnik nieusuwalnych błędów	Wystąpienie nieusuwalnego błędu dysku może następować nie częściej niż 1 na 10^{15} błędów.
Interfejs	Dysk musi być wyposażony w interfejs SAS nie wolniejszy niż 12Gbit/s.

Zabezpieczenia	Dysk musi posiadać co najmniej 2 rodzaje zabezpieczeń w celu ochrony danych.
Gwarancja	Dysk twardy musi posiadać gwarancję nie krótszą niż 2 lat.

Kamery

Kamera tubowa LPR z uchwytami – 2 szt.

Kamera IP	
Typ	Kamera tubowa
Przetwornik	Przetwornik kamery Sony STARVIS nie mniejszy niż 1/2.8” Przetwornik musi być wyposażony w WDR o mocy min. 130dB. Światłoczułość przetwornika 0,02 lx dzień, 0,001 lx noc Rozdzielczość nie mniejsza niż 1920x1080 Zmiennooogniskowy obiektyw pracujący w zakresie min. 2,7 mm do 12 mm wyposażony w Auto Focus, Auto-IRIS Kąty widzenia kamery co najmniej 102 st w poziomie, 58 st w pionie.
Podzespoły	Kamera musi być wyposażona w procesor co najmniej 4 rdzeniowy, z taktowaniem minimalnym 1 GHz per rdzeń Kamera musi posiadać minimum 512 MB pamięci RAM Kamera musi posiadać minimum 256 MB pamięci FLASH
Strumieniowanie	Kamera musi generować 4 strumienie wideo. Przy czym strumień pomocniczy musi być wygenerowany min. w rozdzielczości Full HD. Kamera musi umożliwiać wygenerowanie strumienia MJPEG w rozdzielczości min. FullHD przy odświeżaniu min. 30 kl/s.
Obudowa	Kamera musi posiadać możliwość podłączenia modułu funkcyjnego (np. głośnik, mikrofon). Promiennik powinien pracować na odległość minimum 20m. Doświetlacz powinien być sterowany poprzez samą kamerę wykorzystując sygnał na wejściu alarmowym, zewnętrzną komendę HTTP, poprzez harmonogram. Obudowa kamery powinna posiadać klasę szczelności min. IP67 i klasę wandaloodporności min. IK10. Kamera powinna pracować w zakresie temperatur od -30 do + 50 st C.
Łączność	Kamera musi posiadać protokół ONVIF z profilem G,S,T,M
Kodowanie	Kamera musi obsługiwać kodowanie obrazu H.264 High Profile oraz H.265 (nie dopuszcza się kamer bez wymaganej licencji HEVC Advanced do używania kodeka H.265). Kamera musi obsługiwać kodowanie audio z modulacją G.711/G.726/AAC/LPCM.

Sieć	<p>Kamera powinna posiadać interfejs sieciowy o przepustowości o co najmniej 100Mbps,</p> <p>Obsługiwać protokoły IPv4/v6, TCP, UDP, SNMP, SMTP, RTP, RTSP, HTTP, HTTPS, FTP, NTP, DDNS, SMBv2, AES-256.</p> <p>Kamera musi wspierać wszystkie dostępne na rynku przeglądarki internetowe.</p>
Zabezpieczenia	<p>Kamera musi umożliwiać zarządzanie użytkownikami i grupami ,</p> <p>połączenia SSL, kontrola dostępu oparta na adresie IP, IEEE 802.1X, wykrywanie włamań, cyfrowy podpis obrazu.</p>
Złącza	<p>min. 2 wejścia oraz 1 wyjścia alarmowe, min. 1 wejście oraz 1 wyjście audio, złącze CVBS</p>
Analiza obrazu	<p>Kamera musi umożliwiać odczyt i rozpoznawanie tablic rejestracyjnych (jeżeli wymagana jest dodatkowa licencja, powinna zostać ona uwzględniona w wycenie).</p> <p>Analiza musi być wykonywana przez sieć neuronową na pokładzie kamery.</p> <p>Skuteczność odczytów musi być na poziomie nie mniejszym niż 98%</p> <p>Analiza musi odczytywać tablice rejestracyjne na dwóch pasach jezdni jednocześnie</p> <p>Analiza musi umożliwiać odczyt tablicy rejestracyjnej przy prędkości min. 50 km/h (zadeklarowane przez producenta).</p> <p>Analiza musi umożliwiać kalibrację w postaci ustalenia minimalnej i maksymalnej wielkości znaków.</p> <p>Analiza oprócz rozpoznawania tablic powinna rozpoznawać markę, model oraz kolor pojazdu.</p> <p>Analiza musi umożliwiać integrację z systemami trzecimi i wysyłać metadane przy użyciu XML, JSON, TCP/IP.</p> <p>Kamera powinna rozpoznawać kraj pochodzenia tablicy, a baza krajów powinna zawierać co najmniej 100 krajów.</p>
Funkcjonalności	<p>Kamera musi umożliwiać wysyłanie do innych urządzeń komend CGI,</p> <p>Kamera powinna posiadać panel akcja – reakcja,</p> <p>Wbudowana karta pamięci min. 64 GB,</p> <p>Obsługa kart pamięci o pojemności 1 TB</p> <p>Nagrywanie migawkowe (obrazy przed/po alarmie)</p> <p>Nagrywanie ciągłe</p> <p>Nagrywanie zdarzeń</p> <p>Elastyczna logika zdarzeń sterowana czasem</p> <p>Tygodniowe harmonogramy nagrań i działań</p> <p>Transfer wideo i obrazów ze zdarzeń przez FTP i e-mail</p> <p>Planowanie stref prywatności</p> <p>Zdalne powiadamianie o alarmach (wiadomość sieciowa)</p> <p>Interfejs programowania (HTTP-API)</p> <p>Dioda LED sygnalizująca stan kamery</p>

Atesty	EMC: CE/FCC Safety: LVD
Zasilanie	Kamera musi być zasilana poprzez PoE w standardzie 802.3af Kamera powinna posiadać wsparcie dla trybów A i B PoE Maksymalny pobór prądu nie może przekroczyć 13 W dla zasilania PoE Kamera musi posiadać możliwość zasilenia prądem zmiennym 24V
MTBF	Kamera powinna zapewnić co najmniej 95000 godzin ciągłej pracy
Gwarancja	Kamera powinna posiadać min. 2 lat gwarancji.

Kamera tubowa – szt. 2

Kamera IP	
Typ	Kamera tubowa
Przetwornik	Przetwornik kamery nie mniejszy niż 1/2.8," Rozdzielczość kamery nie mniejsza niż 5MP. Światłoczułość przetwornika nie może być mniejsza niż 0.004 lx w dzień oraz 0.003 w nocy. Kąt widzenia kamery nie może być mniejszy (dopuszcza się szerszy) niż 106° w poziomie oraz 77° w pionie. Kamera musi posiadać zmiennoogniskowy obiektyw o zakresie co najmniej 2,9 mm do 9 mm (dopuszcza się kamery o większym zakresie).
Podzespoły	Kamera musi posiadać wbudowany procesor co najmniej 4 rdzeniowy, o taktowaniu co najmniej 1 GHz per rdzeń.
Strumieniowanie	Kamera musi posiadać moc obliczeniową do generowania co najmniej 4 strumieni wideo. Strumień główny w pełnej rozdzielczości powinien być generowany z odświeżaniem co najmniej 30 kl/s.
Obudowa	Kamera musi posiadać możliwość podłączenia modułu funkcyjnego (np. głośnik, mikrofon). Promiennik powinien pracować na odległość minimum 51m. Doświetlacz powinien być sterowany poprzez samą kamerę wykorzystując sygnał na wejściu alarmowym, zewnętrzną komendę HTTP, poprzez harmonogram. Obudowa kamery powinna posiadać klasę szczelności min. IP66, klasę wandal odporności min. IK10 oraz pyłoszczelność NEMA 4x. Kamera powinna pracować w zakresie temperatur od -30 do + 50 st C.
Łączność	Kamera musi posiadać protokół ONVIF z profilem G,S,T,M Kamera musi znajdować się na liście zintegrowanych natywnie modeli z projektowanym oprogramowaniem.

Kodowanie	<p>Kamera musi obsługiwać kodowanie obrazu H.264 High Profile oraz H.265 (nie dopuszcza się kamer bez wymaganej licencji HEVC Advanced do używania kodeka H.265).</p> <p>Kamera musi obsługiwać kodowanie audio z modulacją G.711/G.726/AAC/</p> <p>Kamera powinna wspierać dwukierunkowe audio.</p> <p>Kamera musi posiadać funkcję inteligentnego kodowania.</p>
Sieć	<p>Kamera musi posiadać interfejs sieciowy o przepustowości co najmniej 100 Mbps.</p> <p>Kamera musi obsługiwać protokoły: IPv6 : TCP/IP, UDP/IP, HTTP, HTTPS, SSL/TLS, SMTP, DNS, NTP, SNMPv1/v2/v3, DHCPv6, RTP, MLD, ICMP, ARP, IEEE 802.1X, Diff Serv, SFTP, MQTT, LLDP IPv4 : TCP/IP, UDP/IP, HTTP, HTTPS, SSL/TLS, RTSP, RTP, RTP/RTCP, SMTP, DHCP, DNS, DDNS, NTP, SNMPv1/v2/v3, UPnP, IGMP, ICMP, ARP, IEEE 802.1X, Diff Serv, SRTP, SFTP, MQTT, LLDP</p>
Zabezpieczenia	<p>Kamera musi umożliwiać zarządzanie użytkownikami i grupami , połączenia SSL, kontrola dostępu oparta na adresie IP, IEEE 802.1X.</p> <p>Kamera musi posiadać certyfikat FIPS 140-2 poziomu trzeciego.</p> <p>Kamera musi być odporna na ataki typu bruteforce.</p>
Złącza	<p>Obsługa min. 2 wejścia oraz 1 wyjścia alarmowe, min. 1 wejście oraz 1 wyjście audio.</p>
Analiza obrazu	<p>Kamera musi posiadać wbudowane algorytmu analizy obrazu, w tym co najmniej:</p> <ul style="list-style-type: none"> – wykrywanie ruchu – wykrywanie dźwięku (np. syrena samochodowa) – wykrycie człowieka wraz z atrybutami (np. kolor ubrania, rodzaj ubrania). – wykrycie pojazdu oraz rodzaju (np. osobowy, ciężarowy itp.) – rozpoznawanie twarzy – anonimizacja twarzy lub całej postury człowieka – wykrycie zmian sceny <p>Do kamery musi zostać dołączona tabela DORI, stworzoną przez producenta kamery.</p> <p>Analiza obrazu musi być zintegrowana z oprogramowaniem działającym u klienta / projektowanym dla klienta.</p>
Funkcjonalności korygujące obraz	<p>Kamera musi być wyposażona w WDR o mocy co najmniej 131 dB.</p> <p>Kamera musi być wyposażona w HLC,</p> <p>Kamera musi być wyposażona BLC,</p> <p>Kamera musi posiadać funkcjonalność kompensacji mgły.</p> <p>Kamera musi posiadać algorytm autokorygujący ustawienia obrazu.</p>
Atesty	<p>UL (UL62368-1), c-UL (CSA C22.2 No.62368-1), CE, IEC62368-1, FCC (Part15 ClassA), ICES-003 ClassA, EN55032 ClassA, EN55035</p>

Zasilanie	Kamera musi być zasilana poprzez PoE w standardzie 802.3af Maksymalny pobór prądu nie może przekroczyć 12 W
Zgodność	Kamera musi być zgodna z ustawą NDAA.
Gwarancja	Kamera musi być objęta co najmniej 2 letnim okresem gwarancyjnym.

Kamera tubowa – 1 szt.

Kamera IP	
Typ	Kamera tubowa
Przetwornik	Przetwornik kamery nie mniejszy niż 1/2.8," Rozdzielczość kamery nie mniejsza niż 8MP. Światłoczułość przetwornika nie może być mniejsza niż 0.02 lx w dzień oraz 0 lx w nocy. Kamera musi posiadać zmiennoogniskowy obiektyw z kątami widzenia nie mniejszymi (dopuszcza się szerszy) niż 112° w poziomie oraz 56° w pionie.
Podzespoły	Kamera musi posiadać wbudowany procesor co najmniej 4 rdzeniowy, o taktowaniu co najmniej 1 GHz per rdzeń.
Strumieniowanie	Kamera musi posiadać moc obliczeniową do generowania co najmniej 4 strumieni wideo. Strumień główny w pełnej rozdzielczości powinien być generowany z odświeżaniem co najmniej 30 kl/s.
Obudowa	Kamera musi posiadać możliwość podłączenia modułu funkcyjnego (np. głośnik, mikrofon). Promiennik powinien pracować na odległość minimum 26m. Doświetlacz powinien być sterowany poprzez samą kamerę wykorzystując sygnał na wejściu alarmowym, zewnętrzną komendę HTTP, poprzez harmonogram. Obudowa kamery powinna posiadać klasę szczelności min. IP66, klasę wandal odporności min. IK10 oraz pyłoszczelność NEMA 4x. Kamera powinna pracować w zakresie temperatur od -30 do + 50 st C.
Łączność	Kamera musi posiadać protokół ONVIF z profilem G,S,T,M Kamera musi znajdować się na liście zintegrowanych natywnie modeli z projektowanym oprogramowaniem.
Kodowanie	Kamera musi obsługiwać kodowanie obrazu H.264 High Profile oraz H.265 (nie dopuszcza się kamer bez wymaganej licencji HEVC Advanced do używania kodeka H.265). Kamera musi obsługiwać kodowanie audio z modulacją G.711/G.726/AAC/ Kamera powinna wspierać dwukierunkowe audio. Kamera musi posiadać funkcję inteligentnego kodowania.

Sieć	<p>Kamera musi posiadać interfejs sieciowy o przepustowości co najmniej 100 Mbps.</p> <p>Kamera musi obsługiwać protokoły: IPv6 : TCP/IP, UDP/IP, HTTP, HTTPS, SSL/TLS, SMTP, DNS, NTP, SNMPv1/v2/v3, DHCPv6, RTP, MLD, ICMP, ARP, IEEE 802.1X, Diff Serv, SFTP, MQTT, LLDP IPv4 : TCP/IP, UDP/IP, HTTP, HTTPS, SSL/TLS, RTSP, RTP, RTP/RTCP, SMTP, DHCP, DNS, DDNS, NTP, SNMPv1/v2/v3, UPnP, IGMP, ICMP, ARP, IEEE 802.1X, Diff Serv, SRTP, SFTP, MQTT, LLDP</p>
Zabezpieczenia	<p>Kamera musi umożliwiać zarządzanie użytkownikami i grupami , połączenia SSL, kontrola dostępu oparta na adresie IP, IEEE 802.1X. Kamera musi posiadać certyfikat FIPS 140-2 poziomu trzeciego. Kamera musi być odporna na ataki typu bruteforce.</p>
Analiza obrazu	<p>Kamera musi posiadać wbudowane algorytmu analizy obrazu, w tym co najmniej:</p> <ul style="list-style-type: none"> – wykrywanie ruchu – wykrywanie dźwięku (np. syrena samochodowa) – wykrycie człowieka – wykrycie pojazdu <p>Do kamery musi zostać dołączona tabela DORI, stworzoną przez producenta kamery.</p> <p>Analiza obrazu musi być zintegrowana z oprogramowaniem działającym u klienta / projektowanym dla klienta.</p>
Funkcjonalności korygujące obraz	<p>Kamera musi być wyposażona w WDR o mocy co najmniej 120 dB.</p> <p>Kamera musi być wyposażona w HLC,</p> <p>Kamera musi być wyposażona BLC,</p> <p>Kamera musi posiadać funkcjonalność kompensacji mgły.</p> <p>Kamera musi posiadać algorytm autokorygujący ustawienia obrazu.</p>
Atesty	<p>UL (UL62368-1), c-UL (CSA C22.2 No.62368-1), CE, IEC62368-1, FCC (Part15 ClassA), ICES-003 ClassA, EN55032 ClassA, EN55035</p>
Zasilanie	<p>Kamera musi być zasilana poprzez PoE w standardzie 802.3af</p> <p>Maksymalny pobór prądu nie może przekroczyć 10 W</p>
Zgodność	<p>Kamera musi być zgodna z ustawą NDAA.</p>
Gwarancja	<p>Kamera musi być objęta co najmniej 2 letnim okresem gwarancyjnym.</p>

Kamera kopulka (garaże) – 3 szt.

Kamera IP	
Typ	Kamera kopulka
Przetwornik	Przetwornik kamery nie mniejszy niż 1/2.8," Rozdzielczość kamery nie mniejsza niż 8MP. Światłoczułość przetwornika nie może być mniejsza niż 0.02 lx w dzień oraz 0 lx w nocy. Kamera musi posiadać zmiennooogniskowy obiektyw z kątami widzenia nie mniejszymi (dopuszcza się szerszy) niż 103° w poziomie oraz 56° w pionie.
Podzespoły	Kamera musi posiadać wbudowany procesor co najmniej 4 rdzeniowy, o taktowaniu co najmniej 1 GHz per rdzeń.
Strumieniowanie	Kamera musi posiadać moc obliczeniową do generowania co najmniej 4 strumieni wideo. Strumień główny w pełnej rozdzielczości powinien być generowany z odświeżaniem co najmniej 30 kl/s.
Obudowa	Kamera musi posiadać możliwość podłączenia modułu funkcyjnego (np. głośnik, mikrofon). Promiennik powinien pracować na odległość minimum 26m. Doświetlacz powinien być sterowany poprzez samą kamerę wykorzystując sygnał na wejściu alarmowym, zewnętrzną komendę HTTP, poprzez harmonogram. Obudowa kamery powinna posiadać klasę szczelności min. IP66, klasę wandal odporności min. IK10 oraz pyłoszczelność NEMA 4x. Kamera powinna pracować w zakresie temperatur od -30 do + 50 st C.
Łączność	Kamera musi posiadać protokół ONVIF z profilem G,S,T,M Kamera musi znajdować się na liście zintegrowanych natywnie modeli z projektowanym oprogramowaniem.
Kodowanie	Kamera musi obsługiwać kodowanie obrazu H.264 High Profile oraz H.265 (nie dopuszcza się kamer bez wymaganej licencji HEVC Advanced do używania kodeka H.265). Kamera musi obsługiwać kodowanie audio z modulacją G.711/G.726/AAC/ Kamera powinna wspierać dwukierunkowe audio. Kamera musi posiadać funkcję inteligentnego kodowania.
Sieć	Kamera musi posiadać interfejs sieciowy o przepustowości co najmniej 100 Mbps. Kamera musi obsługiwać protokoły: IPv6 : TCP/IP, UDP/IP, HTTP, HTTPS, SSL/TLS, SMTP, DNS, NTP, SNMPv1/v2/v3, DHCPv6, RTP, MLD, ICMP, ARP, IEEE 802.1X, Diff Serv, SFTP, MQTT, LLDP IPv4 : TCP/IP, UDP/IP, HTTP, HTTPS, SSL/TLS, RTSP, RTP, RTP/RTCP, SMTP, DHCP, DNS, DDNS, NTP, SNMPv1/v2/v3, UPnP, IGMP, ICMP, ARP, IEEE 802.1X, Diff Serv, SRTP, SFTP, MQTT, LLDP

Zabezpieczenia	Kamera musi umożliwiać zarządzanie użytkownikami i grupami , połączenia SSL, kontrola dostępu oparta na adresie IP, IEEE 802.1X. Kamera musi posiadać certyfikat FIPS 140-2 poziomu trzeciego. Kamera musi być odporna na ataki typu bruteforce.
Analiza obrazu	Kamera musi posiadać wbudowane algorytmu analizy obrazu, w tym co najmniej: <ul style="list-style-type: none"> – wykrywanie ruchu – wykrywanie dźwięku (np. syrena samochodowa) – wykrycie człowieka – wykrycie pojazdu Do kamery musi zostać dołączona tabela DORI, stworzoną przez producenta kamery. Analiza obrazu musi być zintegrowana z oprogramowaniem działającym u klienta / projektowanym dla klienta.
Funkcjonalności korygujące obraz	Kamera musi być wyposażona w WDR o mocy co najmniej 120 dB. Kamera musi być wyposażona w HLC, Kamera musi być wyposażona BLC, Kamera musi posiadać funkcjonalność kompensacji mgły. Kamera musi posiadać algorytm autokorygujący ustawienia obrazu.
Atesty	UL (UL62368-1), c-UL (CSA C22.2 No.62368-1), CE, IEC62368-1, FCC (Part15 ClassA), ICES-003 ClassA, EN55032 ClassA, EN55035
Zasilanie	Kamera musi być zasilana poprzez PoE w standardzie 802.3af Maksymalny pobór prądu nie może przekroczyć 10 W
Zgodność	Kamera musi być zgodna z ustawą NDAA.
Gwarancja	Kamera musi być objęta co najmniej 2 letnim okresem gwarancyjnym.

Kamera multisensoryczna – szt. 1

Kamera IP	
Typ	Kamera multisensoryczna
Przetwornik	Przetworniki kamery nie mniejsze niż 1/2.8” Rozdzielczość kamery nie mniejsza niż 33 Mpix. Światłoczułość przetwornika nie może być mniejsza niż 0.008 lx w dzień oraz 0 lux w nocy. Kąt widzenia sensora nie może być mniejszy (dopuszcza się szerszy) niż 107° w poziomie oraz 56° w pionie. Kamera musi posiadać stałoogniskowe obiektywy (dopuszcza się kamery o większym zakresie). Każdy z przetworników musi posiadać indywidualną możliwość regulowania w poziomie oraz pionie.

Podzespoły	<p>Kamera musi posiadać wbudowany procesor co najmniej 4 rdzeniowy, o taktowaniu co najmniej 1 GHz per rdzeń.</p> <p>Procesor kamery musi posiadać co najmniej 1MB pamięci cache poziomu drugiego.</p>
Strumieniowanie	<p>Kamera musi umożliwiać elastyczną konfigurację trybów (panorama, 360 st, itp.) strumieniowania.</p>
Obudowa	<p>Kamera musi posiadać możliwość podłączenia modułu funkcyjnego (np. głośnik, mikrofon, moduł Wi-Fi).</p> <p>Promiennik powinien pracować na odległość minimum 38m.</p> <p>Doświetlacz powinien być sterowany poprzez samą kamerę wykorzystując sygnał na wejściu alarmowym, zewnętrzną komendę HTTP, poprzez harmonogram.</p> <p>Obudowa kamery powinna posiadać klasę szczelności min. IP67, klasę wandal odporności min. IK10 oraz pyłoszczelność NEMA 4x.</p> <p>Kamera powinna pracować w zakresie temperatur od -40 do + 60 st C.</p>
Łączność	<p>Kamera musi posiadać protokół ONVIF z profilem G,S,T,M</p>
Kodowanie	<p>Kamera musi obsługiwać kodowanie obrazu H.264 High Profile oraz H.265 (nie dopuszcza się kamer bez wymaganej licencji HEVC Advanced do używania kodeka H.265).</p> <p>Kamera musi obsługiwać kodowanie audio z modulacją G.711/G.726/AAC/</p> <p>Kamera powinna wspierać dwukierunkowe audio.</p> <p>Kamera musi posiadać funkcję inteligentnego kodowania.</p>
Sieć	<p>Kamera musi posiadać interfejs sieciowy o przepustowości co najmniej 1000 Mbps.</p> <p>Kamera musi obsługiwać protokoły: DHCPv6, RTP, MLD, ICMP, ARP, IEEE 802.1X, SFTP, MQTT, LLDP, TCP/IP, UDP/IP, HTTP, HTTPS, SSL/TLS, RTSP, RTP, RTP/RTCP,SMTP, DHCP, DNS, DDNS, NTP, SNMPv1/v2/v3, UPnP, IGMP, , DiffServ, SRTP,</p>
Zabezpieczenia	<p>Kamera musi umożliwiać zarządzanie użytkownikami i grupami , połączenia SSL, kontrola dostępu oparta na adresie IP, IEEE 802.1X.</p> <p>Kamera musi posiadać certyfikat FIPS 140-2 poziomu trzeciego.</p> <p>Kamera musi być odporna na ataki typu bruteforce.</p>
Złącza	<p>min. 2 wejścia oraz 1 wyjścia alarmowe, min. 1 wejście oraz 1 wyjście audio.</p>

Analiza obrazu	<p>Kamera musi posiadać wbudowane algorytmy analizy obrazu, w tym co najmniej:</p> <ul style="list-style-type: none"> – wykrywanie ruchu – wykrywanie dźwięku – wykrycie człowieka wraz z atrybutami (np. kolor ubrania, rodzaj ubrania). – wykrycie pojazdu oraz rodzaju (np. osobowy, ciężarowy itp.) – rozpoznawanie twarzy – detekcja zmian <p>Do kamery musi zostać dołączona tabela DORI, stworzoną przez producenta kamery.</p> <p>Analiza obrazu musi być zintegrowana z oprogramowaniem działającym u klienta / projektowanym dla klienta.</p>
Funkcjonalności	<p>Kamera musi być wyposażona w WDR o mocy co najmniej 120 dB.</p> <p>Kamera musi być wyposażona w HLC,</p> <p>Kamera musi być wyposażona BLC,</p> <p>Kamera musi posiadać funkcję kompensacji mgły,</p> <p>Kamera musi posiadać algorytm autokorygujący ustawienia obrazu.</p>
Atesty	UL, CE, FCC, EN 55032 kl.A, EN 55035
Zasilanie	<p>Kamera musi być zasilana poprzez PoE w standardzie 802.3at</p> <p>Maksymalny pobór prądu nie może przekroczyć 26W</p>
Zgodność	Kamera musi być zgodna z ustawą NDAA.
Gwarancja	Kamera musi być objęta co najmniej 2 letnim okresem gwarancyjnym.

Kamera multisensoryczna – 1 szt.

Kamera IP	
Typ	Kamera multisensoryczna
Przetwornik	<p>Przetworniki kamery nie mniejsze niż 1/2.7"</p> <p>Rozdzielczość kamery nie mniejsza niż 8 Mpix.</p> <p>Światłoczułość przetwornika nie może być mniejsza niż 0.020 lx w dzień oraz 0 lux w nocy.</p> <p>Kąt widzenia kamery nie może być mniejszy (dopuszcza się szerszy) niż 100° w poziomie oraz 56° w pionie.</p> <p>Kamera musi posiadać zmiennogniskowe obiektywy o zakresie co najmniej 3 mm do 7 mm (dopuszcza się kamery o większym zakresie).</p> <p>Każdy z przetworników musi posiadać indywidualną możliwość regulowania w poziomie oraz pionie.</p>
Podzespoły	Kamera musi posiadać wbudowany procesor co najmniej 4 rdzeniowy, o taktowaniu co najmniej 1 GHz per rdzeń.

Strumieniowanie	<p>Kamera musi posiadać moc obliczeniową do generowania co najmniej 4 strumieni wideo.</p> <p>Strumień główny w pełnej rozdzielczości powinien być generowany z odświeżaniem co najmniej 30 kl/s.</p>
Obudowa	<p>Kamera musi posiadać możliwość podłączenia modułu funkcyjnego (np. głośnik, mikrofon, moduł Wi-Fi).</p> <p>Promiennik powinien pracować na odległość minimum 40m.</p> <p>Doświetlacz powinien być sterowany poprzez samą kamerę wykorzystując sygnał na wejściu alarmowym, zewnętrzną komendę HTTP, poprzez harmonogram.</p> <p>Obudowa kamery powinna posiadać klasę szczelności min. IP67, klasę wandal odporności min. IK10 oraz pyłoszczelność NEMA 4x.</p> <p>Kamera powinna pracować w zakresie temperatur od -40 do + 60 st C.</p>
Łączność	Kamera musi posiadać protokół ONVIF z profilem G,S,T,M
Kodowanie	<p>Kamera musi obsługiwać kodowanie obrazu H.264 High Profile oraz H.265 (nie dopuszcza się kamer bez wymaganej licencji HEVC Advanced do używania kodeka H.265).</p> <p>Kamera musi obsługiwać kodowanie audio z modulacją G.711/G.726/AAC/</p> <p>Kamera powinna wspierać dwukierunkowe audio.</p> <p>Kamera musi posiadać funkcję inteligentnego kodowania.</p>
Sieć	<p>Kamera musi posiadać interfejs sieciowy o przepustowości co najmniej 1000 Mbps.</p> <p>Kamera musi obsługiwać protokoły: DHCPv6, RTP, MLD, ICMP, ARP, IEEE 802.1X, SFTP, MQTT, LLDP, TCP/IP, UDP/IP, HTTP, HTTPS, SSL/TLS, RTSP, RTP, RTP/RTCP,SMTP, DHCP, DNS, DDNS, NTP, SNMPv1/v2/v3, UPnP, IGMP, , DiffServ, SRTP,</p>
Zabezpieczenia	<p>Kamera musi umożliwiać zarządzanie użytkownikami i grupami , połączenia SSL, kontrola dostępu oparta na adresie IP, IEEE 802.1X.</p> <p>Kamera musi posiadać certyfikat FIPS 140-2 poziomu trzeciego.</p> <p>Kamera musi być odporna na ataki typu bruteforce.</p>
Złącza	Obsługa min. 2 wejścia oraz 1 wyjścia alarmowe, min. 1 wejście oraz 1 wyjście audio.
Analiza obrazu	<p>Kamera musi posiadać wbudowane algorytmy analizy obrazu, w tym co najmniej:</p> <ul style="list-style-type: none"> – wykrywanie ruchu – wykrywanie dźwięku – wykrycie człowieka wraz z atrybutami (np. kolor ubrania, rodzaj ubrania). – wykrycie pojazdu oraz rodzaju (np. osobowy, ciężarowy itp.) – rozpoznawanie twarzy – detekcja zmian

	Do kamery musi zostać dołączona tabela DORI, stworzoną przez producenta kamery. Analiza obrazu musi być zintegrowana z oprogramowaniem działającym u klienta / projektowanym dla klienta.
Funkcjonalności	Kamera musi być wyposażona w WDR o mocy co najmniej 100 dB. Kamera musi być wyposażona w HLC, Kamera musi być wyposażona BLC, Kamera musi posiadać funkcję kompensacji mgły, Kamera musi posiadać algorytm autokorygujący ustawienia obrazu.
Atesty	UL, CE, FCC, EN 55032 kl.A, EN 55035
Zasilanie	Kamera musi być zasilana poprzez PoE w standardzie 802.3at Maksymalny pobór prądu nie może przekroczyć 23 W
Zgodność	Kamera musi być zgodna z ustawą NDAA.
Gwarancja	Kamera musi być objęta co najmniej 2 letnim okresem gwarancyjnym.

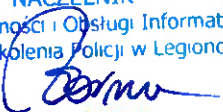
Dodatkowe wymagania:


I. Wykonawca powinien posiadać następujące certyfikaty lub równoważne w zakresie min. :

1. Certyfikat **ISO 9001** zarządzanie jakością w zakresie przedmiotowym oferty:
 - jakości sprzedaży systemów informatycznych oraz technicznych systemów bezpieczeństwa
 - Projektowanie, sprzedaż i wdrażanie rozwiązań informatycznych do zarządzania technicznymi systemami bezpieczeństwa
 - Dostarczanie usług serwisowych do rozwiązań informatycznych i technicznych systemów bezpieczeństwa
2. Certyfikat **ISO 27 001** zarządzanie bezpieczeństwem informacji w zakresie przedmiotu oferty:
 - Sprzedaż technicznych systemów bezpieczeństwa
 - Projektowanie, sprzedaż i wdrażanie rozwiązań informatycznych do zarządzania technicznymi systemami bezpieczeństwa
 - Dostarczanie usług serwisowych do rozwiązań informatycznych i technicznych systemów bezpieczeństwa
3. Certyfikat **ISO 20 000** zarządzanie usługami IT w zakresie przedmiotu oferty:
 - Sprzedaż technicznych systemów bezpieczeństwa
 - Projektowanie, sprzedaż i wdrażanie rozwiązań informatycznych do zarządzania technicznymi systemami bezpieczeństwa
 - Dostarczanie usług serwisowych do: rozwiązań informatycznych technicznych systemów bezpieczeństwa.

II. Wykonawca powinien posiadać wiedzę i doświadczenie w zakresie instalowania oferowanego oprogramowania.

III. Wykonawca powinien posiadać autoryzacje na sprzedaż i wdrażanie Producenta oferowanego oprogramowania.


 NACZELNIK
 Wydziału Łączności i Obsługi Informatycznej
 Centrum Szkolenia Policji w Legionowie
 Joanna ZARNA


 NACZELNIK
 Wydziału Inwestycji i Remontów
 Centrum Szkolenia Policji w Legionowie
 Agnieszka CHOJECKA

Dokumentacja fotograficzna



