# Minimalne wymagania techniczne które musi spełniać oprogramowania do zarządzania systemem monitoringu CCTV w wersji IP dla Aresztu Śledczego w Piotrkowie Trybunalskim

# Spis treści

# 1. Oprogramowanie do Zarządzania Bezpieczeństwem – wymagania

Oprogramowanie do Zarządzania Bezpieczeństwem musi być oprogramowaniem klasy korporacyjnej umożliwiającym bezproblemowe połączenie w ramach wspólnej platformy i jednorodnego interfejsu: systemu automatycznego rozpoznawania tablic rejestracyjnych (LPR), systemu kontroli dostępu (KD), systemu zarządzania video (VMS) i systemu sygnalizacji włamania i napadu. Aplikacje interfejsu użytkownika (UI) powinny przedstawiać zunifikowany interfejs bezpieczeństwa do zarządzania, konfiguracji, monitorowania i raportowania wbudowanych systemów oraz powiązanych urządzeń brzegowych.

Oprogramowanie musi być produktem istniejącym (typu box) oferującym opisane funkcjonalności, które są już wdrożone na innych obiektach i możliwe do zweryfikowania.

Informacje na temat warunków gwarancyjnych oraz wymagań systemowych oprogramowania powinny być dostępne publicznie na stronie internetowej producenta.

W celu zachowania zasad rynkowej konkurencji producent oprogramowania powinien dysponować oficjalną siecią partnerską/dystrybucyjną, w tym minimum dwoma dystrybutorami na terenie Polski.

## 1.1. Podstawowe Funkcje Oprogramowania do Zarządzania Bezpieczeństwem:

Zarządzanie i konfiguracja systemów wbudowanych, takich jak LPR, KD i VMS.

Monitorowanie, raportowanie i zarządzanie alarmami wielu zdalnych i niezależnych systemów LPR, KD i VMS rozmieszczonych w wielu obiektach i obszarach geograficznych zbudowanych w oparciu o oprogramowanie producenta.

Integracja urządzeń i systemów antywłamaniowych (monitorowanie na żywo, raportowanie oraz uzbrojenie / rozbrojenie), z obsługą z poziomu aplikacji klienckiej.

Integracja z systemami i bazami danych innych firm za pośrednictwem wtyczek w tym z: systemami kontroli dostępu, analityką video, systemami antywłamaniowymi, systemami ochrony obwodowej i innymi.

Integracja z systemami automatyki z obsługą protokołów komunikacyjnych modbus i bacnet.

Integracja z systemami Advisor Master i Advisor Advanced.

Integracja z serwerami i klientami OPC (OLE for Process Control).

Oprogramowania do Zarządzania Bezpieczeństwem musi być kompatybilne ze środowiskami wirtualnymi, w tym VMware i Microsoft Hyper-V.

## 1.2. Architektura

Oprogramowanie platformy 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.

Platforma musi bazować na rozwiązaniach IP. Cała komunikacja między serwerem a aplikacją kliencką oparta jest na standardowym protokole TCP/IP wraz z możliwością uruchomienia szyfrowania TLS z cyfrowymi certyfikatami w celu zabezpieczenia kanału komunikacji.

Oprogramowanie serwera pracuje jako usługa Windows w taki sposób, aby uruchamiała się wraz ze startem systemu operacyjnego i pracowała w tle

Wiele obiektów zbudowanych w oparciu o opisane oprogramowanie musi mieć możliwość połączenia w jeden duży wirtualny system scentralizowanego monitorowania, raportowania i zarządzania alarmami.

W systemie musi być możliwość wyróżnienia następujących modułów/funkcjonalności:

A. Serwer centralny, który musi zarządzać główną bazą danych, autoryzować użytkowników, zarządzać komponentami w podsystemach.
B. Serwer pełniący funkcję rejestratora, który jest odpowiedzialny za zarządzanie przydzielonymi kamerami i koderami oraz archiwizowanie video.
C. Serwer odpowiedzialny za przesyłanie video i audio przez sieci lokalne i rozległe (LAN, Internet) ze źródła video (kamera IP, enkoder) do miejsca docelowego (np. aplikacji klienckiej)

Oprogramowanie musi umożliwiać wydzielenie fizycznych urządzeń/serwerów pełniących powyższe funkcje (serwera zarządzającego, rejestrującego, przesyłającego)

Każda z funkcji (serwer zarządzający, rejestrujący, przesyłający), w razie potrzeby, musi mieć własną bazę danych do przechowywania zdarzeń i informacji konfiguracyjnych dotyczących określonej roli.

### 1.3. Dynamiczne mapy

System musi obsługiwać funkcje mapowania dla kontroli dostępu, nadzoru video, wykrywania włamań, LPR i aplikacji zewnętrznych, musi zawierać interfejs zorientowany na mapę z możliwością dowodzenia i kontrolowania wszystkich jego możliwości z pełnoekranowego interfejsu mapy.

System musi obsługiwać następujące formaty plików i protokoły do importowania tła mapy: Pdf, Jpg, Png, Usługa Web Tile Map Service (WMTS) i Web Map Service (WMS) zdefiniowane przez Open GeospatialConsortium (OGC), BeNomad (BeNomad) , AutoCAD (DWG i DXF).

System musi zapewniać możliwość wyświetlania wszystkich zaimplementowanych obiektów, w tym:

A. Kamery, Stałopozycyjne, PTZ,LPR, sekwencje kamer
B. Drzwi
C. Obszary
D. Obszary i strefy ochrony antywłamaniowej
E. Wejścia i wyjścia cyfrowe
F. Interkomy
G. Alarmy
H. Makra

System musi zapewnić możliwość rysowania i wyświetlania informacji na mapie w postaci takich jak: kształty wektorowe: linia, prostokąty, wielokąty, elipsa, zdjęcia, tekst.

System musi umożliwiać monitorowanie stanu obiektów na mapie. Musi być możliwe dostosowanie ikon dowolnych obiektów reprezentowanych na mapie.

System musi oferować narzędzie inteligentnego wyboru w celu uzyskania dostępu do video. Klikając lokalizację, którą użytkownik chce zobaczyć, system automatycznie wybierze kamery, które mogą zobaczyć tę lokalizację i przesuną PTZ w kierunku tej lokalizacji. Narzędzie wyboru musi brać pod uwagę przeszkody i nie wyświetlać kamer, które nie widzą lokalizacji z powodu ściany (przeszkody), która przysłania obraz.

Graficzny interfejs map musi oferować możliwość pełnego działania funkcji monitorowania alarmów. W tym takich funkcji jak:

A. Wyśrodkuj mapę na obiektach związanych z alarmem.
B. Uwidocznij powiadomienia Alarmowe na mapie i uzyskaj dostęp do powiązanych filmów z mapy.
C. Wyzwalaj i odbieraj alarmy.

D. Działaj w sprawie otrzymanego alarmu, w tym wyślij potwierdzenie odebrania alarmu, prześlij alarm dalej i rozpocznij obsługę alarmu.
E. Uwidocznij fakt, że wystąpił alarm na połączonej mapie w tle.

System musi umożliwiać dodanie zaawansowanej funkcjonalności do map obiektów za pomocą SDK.

### 1.4. Wymagania cyberbezpieczeństwa

Cała komunikacja między serwerem, a klientem, a więc strumienie mediów, w tym video, audio i metadane, musi być oparta na standardowym protokole TCP/IP i wykorzystywać szyfrowanie TLS z cyfrowymi certyfikatami. VMS musi obsługiwać tylko zabezpieczone żądania strumienia mediów, chyba, że wyraźnie skonfigurowano inaczej. Żądania strumienia mediów muszą być zabezpieczone silnym uwierzytelnianiem opartym na certyfikatach wykorzystującym RTSPS (RTSP przez TLS).Szyfrowanie strumienia multimediów powinno odbywać się w spoczynku i podczas transportu i powinno być oparte na certyfikacie szyfrowania bitów AES 128.

Oprogramowanie serwera musi zapewniać Administratorowi możliwość konfiguracji portów.

Oprogramowanie serwera powinno przedstawiać zalecenia dotyczące haseł używanych do uzyskiwania dostępu do jednostek sprzętowych w systemie (kamery, kontrolery, enkodery itp.). Zalecenia powinny klasyfikować hasła używane w jednostkach jako: słabe, średnie, silne lub bardzo silne.

Oprogramowanie serwera powinno weryfikować i publikować informacje dotyczące oprogramowania układowego urządzeń pracujących w systemie, z kwalifikacją czy oprogramowanie układowe jest aktualne i czy aktualizacja jest zalecana, czy wymagana.

### 1.5. Kontrola pracy operatora i procedury operacyjne

System musi umożliwiać przeprowadzenie audytu aktywności Użytkownika (w formie dziennika), audyty muszą być generowane jako raporty. Muszą przedstawiać czynności wykonane w określonych przedziałach czasowych, przez konkretnych użytkowników, wskazywać wprowadzone w systemie zmiany, obiekty, których dotyczy problem i okresy czasowe.

System musi wspierać generowanie ścieżek aktywności użytkownika. Ścieżki aktywności użytkownika muszą składać się z dzienników aktywności operatora, takich jak logowanie, przeglądanie kamery, przeglądanie zdarzenia LPR, drukowanie identyfikatorów, eksport video.

System musi umożliwiać operatorowi tworzenie raportów ze zdarzeń, które miały miejsce podczas jego zmiany. Obsługiwane muszą być zarówno raporty o zdarzeniach związanych z video, jak i kontrolą dostępu.

System musi umożliwiać zdalne monitorowania i kontrolowania zawartości innych stacji roboczych, które są częścią tego samego systemu.

W celu automatyzacji reakcji na typ zdarzenia system musi mieć możliwość wbudowania narzędzia do organizacji pracy operatorów zgodnie z wprowadzonymi procedurami operacyjnymi.

### 1.6. Ochrona prywatności i danych osobowych w monitoringu video

VMS musi mieć możliwość automatycznego zasłaniania/maskowania osób i pojazdów w ruchu, w nagraniach video i w czasie rzeczywistym.

Funkcja musi maskować ruchy za pomocą bloków, zasłaniając w ten sposób kontur obiektu lub osoby. Strefy maskowania muszą być dowolnie definiowanymi wielokątami.

Funkcja maskowania osób i pojazdów musi pracować w trybach wewnętrznym i zewnętrznym.

Funkcjonalność maskowania osób i pojazdów musi być realizowana na serwerze bez konieczności obliczeń w kamerze. Obraz ma być maskowany w trybie live/zapis tak żeby użytkownik o odpowiednich uprawnieniach miał możliwość usunięcia maskowania. Dotyczy to zarówno materiału video już zarejestrowanego jak i przeglądanego na żywo.

Zdjęcie/usunięcie maskowania musi być możliwe wyłącznie dla administratorów/operatorów z odpowiednimi uprawnieniami.

## 2. Funkcjonalność oprogramowania VMS– wymagania:

Budowa platformy VMS zakłada dostawę, instalację oraz uruchomienie (na serwerach rejestracji i zarządzania wideo) oprogramowania do rejestracji i zarządzania wideo. Platforma VMS jest rozwiązaniem programowym bazującym na architekturze IP.

### 2.1. Podstawowe wymagania oprogramowania platformy VMS:

- Wyświetlanie strumieni wideo na żywo
- Rejestracja strumieni wideo
- Monitorowanie na żywo strumieni z kamer oraz dostęp do zarejestrowanego materiału wideo
- Monitorowanie zdarzeń na żywo
- Zarządzanie alarmami
- Raportowanie, włącznie z tworzeniem własnych szablonów raportów oraz raportowaniem incydentów
- Integrację z Microsoft Active Directory dla synchronizacji kont użytkowników
- Nadzór / konfiguracja poprzez klientów www
- Obsługa zaawansowanej analityki wideo (po stronie kamer)
- Obsługa analityki wideo pochodzącej od zewnętrznych dostawców (co najmniej 5 różnych dostawców)
- Monitorowanie stanu systemu
- Zarządzanie kontami użytkowników i administratorów
- Zarządzanie prawami dostępu do systemu dla użytkowników lokalnych i zdalnych
- Zarządzanie prawami dostępu do materiałów wideo dla użytkowników lokalnych i zdalnych
- Zarządzanie priorytetami dostępu i sterowania w oparciu o priorytety kont użytkowników
- Integracja z różnymi kamerami IP oraz klawiaturami IP

**Oprogramowanie VMS musi być przewidziane do współpracy z oprogramowaniem Microsoft. Należy dostarczyć dokument potwierdzający ww. Np. Microsoft Gold Certified Partner – certyfikat dla oprogramowanie do rejestracji i zarządzania wideo.**

### 2.2. Licencjonowanie

- Pojedyncza licencja jest stosowana na centralnym serwerze odpowiedzialnym za konfigurację.
- Nie ma konieczności stosowania licencji na stacji klienckiej.

### 2.3. Sprzęt i oprogramowanie

- Oprogramowanie VMS zaprojektowane do uruchamiania na typowej platformie PC pracującej pod kontrolą systemu operacyjnego Windows.
- Moduł oprogramowania serwerowego musi być kompatybilny z 32 oraz 64 bitowymi wersjami systemów Windows, włączając Windows 10, Windows 11, Windows Server 2016, Windows Server 2022.
- Moduł oprogramowania serwerowego musi posiadać pełne wsparcie dla wirtualizacji
- Moduł oprogramowania klienckiego jest kompatybilny z Windows 10, Windows 11.

### 2.4. Skalowalność platformy VMS

Architektura platformy VMS powinna umożliwiać pełną skalowalność, i ma umożliwiać rozbudowę systemu do co najmniej: 50 serwerów rejestracji i zarządzania, 100 stacji klienckich, 1000 kamer, 500 modułów wejść/wyjść alarmowych.

### 2.5. Standardowe funkcjonalności platformy VMS

- W systemie można wyróżnić serwer centralny który zarządza główną bazą danych, zawierającą wszystkie informacje o systemie i konfiguracji komponentów platformy VMS. Serwer ten autoryzuje użytkowników i nadaje dostęp do platformy na podstawie predefiniowanych praw dostępu użytkownika oraz ustawień strefy bezpieczeństwa. Serwer z taką funkcjonalnością konfiguruje/zarządza m.in. następującymi komponentami w podsystemach VMS:
    - Podział logiczny jednego systemu na kilka podsystemów (np. partycje)
    - użytkownicy i grupy użytkowników
    - wejścia/wyjścia (IO),
    - alarmy
    - zdarzenia własne
    - makra oraz skrypty własne.
- Serwer centralny może konfigurować/zarządzać następującymi komponentami VMS:
    - Enkodery wideo i ich urządzenia zewnętrzne np. audio, porty WE/WY, porty szeregowe
    - sterowanie PTZ
    - Sekwencje kamer
    - Harmonogramy nagrywania i archiwizacji.
- W platformie VMS można wyróżnić funkcjonalność rejestratora która jest odpowiedzialna za zarządzanie przydzielonymi kamerami i koderami oraz archiwizowanie wideo.
- W platformie VMS można wyróżnić serwer odpowiedzialny za przesyłanie wideo i audio przez sieci lokalne i rozległe (LAN, Internet) ze źródła video (kamera IP, enkoder) do miejsca docelowego (np. aplikacji klienckiej)
- W platformie VMS musi znajdować się funkcjonalność, która monitoruje i zapisuje zdarzenia stanu systemu oraz ostrzeżenia z różnych aplikacji klienta, usług, które są częścią platformy VMS. Funkcjonalność ta generuje raporty statystyk dotyczących stanu i historii stanu systemu
- Platforma VMS musi umożliwiać tworzenie i zarządzanie ścianą wideo, poprzez zastosowania stacji komputerowych typu desktop i dołączonych monitorów bezszwowych, zamiast dedykowanego rozwiązania dla ścian wideo
- Platforma VMS musi umożliwiać przechwytywanie pułapek w standardzie SNMP w sieci TCP/IP generowanych przez urządzenia znajdujące się w sieci. Przechwytywanie musi odbyć się przez platformą lub dodatkową aplikację (nie koniecznie od tego samego producenta) zainstalowaną na serwerze systemowym. Platforma musi umożliwiać przetworzenie złapanych pułapek SNMP na zdarzenia systemowe i na ich podstawie przykładowo wywołać alarm

### 2.6. Usługa Monitorująca działanie serwerów platformy cyfrowej (Watchdog).

- Platforma cyfrowa zawiera usługę Monitorującą Pracę Serwerów (Watchdog), która nieprzerwanie monitoruje stan usług serwerów
- Usługa Monitorująca Pracę Serwerów instalowana jest na wszystkich serwerach/komputerach, na których działa serwer VMS. W wypadku błędu lub awarii, Watchdog restartuje usługę, w której wystąpił błąd. W ostateczności, Watchdog uruchamia serwer/komputer ponownie, jeśli nie jest w stanie uruchomić ponownie usługi.

### 2.7. Aplikacja kliencka.

- Aplikacja kliencka zapewnia interfejs użytkownika dla konfiguracji i monitorowania w dowolnej sieci, dostępnej lokalnie lub poprzez połączenie zdalne.
- Wszystkie aplikacje posiadają 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 przebiega poprzez konta i hasła platformy przechowywane lokalnie lub poprzez uwierzytelnienia użytkownika Windows, gdy integracja z Active Directory jest włączona.
- Aplikacja musi mieć możliwość wymuszenia na użytkowniku logowanie się razem z jego przełożonym lub administratorem, posiadającym wyższe prawa w hierarchii systemu.

- Aplikacja kliencka dostępna jest w języku polskim,
- W celu usprawnienia użytkowania i efektywności w aplikacji klienckiej zaimplementowano dla czynności administrator/użytkownik podejście zorientowane zadaniowo. Operator może uruchomić określone zadanie tylko, jeśli posiada do tego określone uprawnienia. Poprzez wykorzystanie uprawnień możliwe jest ukrywanie zadań, do których operator nie może mieć dostępu.

Należy zastosować oprogramowanie stanowiące graficzny interfejs mapy. Graficzny interfejs mapy może być niezależnym, rozbudowanym narzędziem, które będzie zintegrowane z oprogramowaniem do zarządzania i rejestracji wideo. Graficzny interfejs mapy musi spełniać co najmniej następujące wymagania dla oprogramowania stacji klienckiej:

- Wyświetlanie wielu map dla jednego oraz dla wielu obszarów,
- Wyświetlanie map jako warstw,
- Wyświetlanie podkładów mapowych w postaci map GIS
- Wyświetlanie podkładów mapowych w postaci bitmap,
- Przełączanie się pomiędzy mapami: poprzez wybór warstwy, poprzez aktywne przyciski,
- Wyświetlanie na mapie aktywnych ikon urządzeń w systemie,
- Wyświetlanie na mapie aktywnych obszarów obserwacji kamer stacjonarnych w systemie,
- Wyświetlanie na mapie aktywnych obszarów obserwacji kamer obrotowych w systemie (poprzez wskazanie aktualnego kierunku obserwacji kamery obrotowej - wyświetlenie płynnie zmieniającego się pola widzenia kamery obrotowej - pokazanie rzeczywistego kierunku i zakresu obserwacji z kamery),
- Wyświetlanie na mapie aktywnych ikon urządzeń powiązanych z alarmami,

Oprogramowanie stacji klienckiej umożliwi zastosowanie modułu konfiguratora do zarządzania, konfiguracji oprogramowania, do nadzoru oraz do automatycznego i ręcznego raportowania stanu systemu oraz stanu urządzeń peryferyjnych.

### 2.8. Aplikacja kliencka. Panel monitoringu/dozoru

- Panel monitoringu/dozoru musi posiadać graficzny interfejs użytkownika do kontroli i monitorowania platformy bezpieczeństwa z dowolnej sieci IP. Umożliwia administratorowi i operatorom o odpowiednich przywilejach monitorowanie, uruchamianie raportów i zarządzanie alarmami.
- Panel monitoringu/dozoru posiada następujące opcje usprawniania użytkowania i efektywności działania, takie jak :
    - Dynamicznie adaptowalny interfejs użytkownika, który dopasowuje się w czasie rzeczywistym do tego, co robi operator.
    - Dynamiczny panel sterowania wypełniony widgetami specyficznymi dla obiektu, np. kamer.
    - Wykorzystanie półprzezroczystych nakładek, które wyświetlają wiele danych w nieprzeszkadzający sposób.
    - Menu w okienkach układu i szybkie polecenia łatwo dostępne z każdej części pulpitu użytkownika.
- Dynamicznie adaptowane interfejs użytkownika, panel zadań i widgety
    - Panel Dozoru dostosowuje się dynamicznie do działań operatora. Przeprowadzane jest to za pomocą widgetów zgrupowanych w panelu zadań panelu monitoringu/dozoru.
    - Widgety to mini-aplikacje lub mini-grupy w panelu monitoringu/dozoru, które umożliwiają wykonywanie częstych zadań i nadają szybki dostęp do informacji i działań.
    - Jedno kliknięcie na jednostkę (np. kamery) wywołuje na ekran określony widget powiązany z tą jednostką a inne niepowiązane widgety znikają dynamicznie. Widgety zawierają informacje takie jak informacje o transmisji wideo, a także o działaniach użytkownika, takich jak kontrole PTZ i inne.
    - Określone widgety przypisane są do kamer, alarmów, stref, ekranów, transmisji wideo (statystyki), kamer PTZ i innych.
- Każde zadanie aplikacji klienckiej zawiera jedno lub więcej następujących elementów:
    - Lista zdarzeń.
    - Drzewo logiczne: kamer, stref, zgrupowanych hierarchicznie zgodnie ze strefami do których należą w podległy sposób.
    - Ekrany o wielu układach (1 x 1, 2 x 2, 3x3, 8x8)

- Panel sterowania
- Wyświetlane menu z różnymi poleceniami związanymi z kamerami, PTZ i kontrolą ekranu

- Panel monitoringu/dozoru zapewnia wiele list zdarzeń i wyświetlania pól, w tym:
  - Widok samej listy zdarzeń/alarmów
  - Widok samych układów
  - Widok łączony układów oraz listy alarmów/zdarzeń
- Dostosowanie panelu pracy użytkownika
  - Użytkownik posiada pełną kontrolę nad panelem użytkownika poprzez wiele opcji konfiguracji wybieranych ręcznie
  - Po przeprowadzeniu dopasowania, użytkownik może zapisać swój panel.
  - Panel dostępny jest dla konkretnego użytkownika z dowolnej aplikacji klienta w sieci (dowolnej stacji).
  - Układy ekranów są modyfikowalne.
  - Panel Dozoru może pracować na tak wielu monitorach, ile akceptuje karta grafiki komputera PC oraz system operacyjny Windows.
- Panel Dozoru zawiera zaawansowane opcje wideo:
  - Zaawansowany podgląd wideo na żywo.
  - Zaawansowane odtwarzanie z archiwów i bieżący przegląd zapisanego wideo.
  - Monitorowanie i zarządzanie zdarzeniami i alarmami systemu wideo.
  - Tworzenie raportów wideo.
  - Sterowanie kamerami PTZ.
- Opcje podglądu na żywo Panelu Dozoru to:
  - Wyświetlanie wszystkich kamer platformy VMS i wszystkich kamer połączonych ze sfederowanymi systemami.
  - Monitorowanie wideo na żywo na każdym ekranie z osobna w zakresie jednego zadania w panelu użytkownika.
  - Operator przeciąga kamerę na ekran w celu włączenia odtwarzania na żywo.
  - Operator przeciąga kamerę z mapy na ekran w celu włączenia odtwarzania na żywo.
  - Operator może kierować ruchem kamery, zoomem, przesłoną, ostrością i wywoływać presety.
  - Operator może oznaczyć ważne zdarzenia do przejrzenia później w dowolnej kamerze archiwizującej. Operator może nadać nazwę każdej zakładce, aby ułatwić późniejsze wyszukiwanie.
  - Operator może zatrzymać/uruchomić nagrywanie z dowolnej kamery w systemie, która jest skonfigurowana w sposób umożliwiający nagrywanie ręczne poprzez kliknięcie w jeden guzik.
  - Operator może przejść do odtwarzania wideo z każdej kamery archiwizującej dzięki tylko jednemu kliknięciu.

**Opcje odtwarzania wideo z aplikacji klienckiej z panelu monitoringu (przegląd archiwum) obejmują:**

- Odtwarzanie audio i wideo z dowolnego zakresu czasuna dowolnym ekranie.
- Wybór pomiędzy odtwarzaniem niezsynchronizowanym lub natychmiastową synchronizacją wszystkich strumieni wideo w trybie odtwarzania,
- Jednoczesne odtwarzanie tej samej kamery na wielu ekranach w różnych przedziałach czasowych.
- Wyświetlanie pojedynczego paska czasu lub jednego paska czasu dla każdej wybranej sekwencji wideo,
- Wyświetlanie wielkości (poziomu) ruchu w dowolnym przedziale czasu.
- Wyszukuje zarchiwizowane wideo za pomocą zapytań i różnych kryteriów wyszukiwania, w tym czasu, daty, kamery, obszaru i innych.
- Udostępnia narzędzie wyszukiwania zdarzeń zdefiniowanych przez użytkownika lub według parametrów detekcji ruchu pośród plików wideo i powiązanych plików dźwiękowych.
- Dodawanie zakładek do wcześniej nagranego wideo w celu łatwiejszego wyszukiwania i selekcji.
- Eksportowanie zdjęć w formacie PNG, JPEG, GIF i BMP z oznaczeniem daty i czasu, a także nazwą kamery na obrazie (stop klatek).
- Eksportowanie sekwencji video i audio w standardowych formatach wideo np. ASF oraz formatu natywnego producenta platformy ze znacznikami daty i czasu w obrazie. Możliwe jest szyfrowanie eksportowanych

sekwencji video. Możliwość dodawanie zabezpieczenia w postaci tzw. znaku wodnego do eksportowanego materiału.
- Narzędzia do eksportu wideo na różnych nośnikach, takich jak CD-ROM.

### 2.9. Praca awaryjna (Failover) i czuwanie (Standby)

- Platforma bezpieczeństwa obsługuje własne, a także standardowe opcje pracy w przypadku wystąpienia awarii (failover).
- Praca w trybie awarii centralnego serwera
    - Zapasowy server centralny (standby) działa jako serwer zastępczy pracując w trybie czuwania, będąc gotowym do przejęcia pracy jako serwercentralny w razie awarii głównego serwera centralnego. Przejęcie nastąpi w czasie krótszym niż 2 minuty. Nie wymaga to ingerencji użytkownika.
    - Platforma bezpieczeństwa obsługuje do pięciu serwerów centralnych w trybie czuwania, oczekujących w kolejce do przejęcia funkcji bieżącego, głównego serwera centralnego w sposób kaskadowy.
    - Zapasowy serwer centralny zachowuje bazę danych konfiguracji zsynchronizowaną z głównym serwerem centralnym,

### 2.10. Integracja z systemami firm trzecich

- Platforma bezpieczeństwa oferuje wiele możliwości integracji z systemami firm obcych. Wśród nich: Software Development Kits (SDK), Driver Development Kits (DDK), Web Service SDK
- Platforma bezpieczeństwa umożliwia dodanie nowych łączników integrujących systemy zewnętrzne, takich jak: analityka wideo, zewnętrzne systemy wideo firm obcych, zarządzanie alarmami

### 2.11. Monitoring funkcjonowania platformy VMS

- Platforma monitoruje stan systemu, zapisuje zdarzenia związane ze stanem sprawności i oblicza statystyki.
- Usługi platformy, role, jednostki i aplikacje klienta wywołują zdarzenia związane ze stanem sprawności.
- Zadanie Monitorowania kondycji platformy i raport historii kondycji są dostępne dla raportowania na żywo i w odniesieniu do czasu przeszłego.

### 2.12. Zaawansowane Zarządzanie Zadaniami

- Administrator może przypisywać zadania i blokować pulpit operatora. Zarządzanie swoim pulpitem przez użytkownika może być ograniczone przez przydzielone uprawnienia.
- Operatorzy mogą zapisywać swoje zadania jako zadania publiczne lub prywatne w określonych partycjach systemu. Zadania publiczne są dostępne dla wszystkich użytkowników. Zadania prywatne są widoczne tylko dla właściciela zadania.
- Operatorzy mogą udostępniać zadania poprzez wysyłanie ich do jednego lub więcej podłączonych aktualnie użytkowników. Zadanie może zostać wysłane na wskazany przez operatora monitor użytkownika. Odbiorcy mają następnie możliwość przyjęcia takiego zadania.

### 2.13. Raportowanie

- Platforma umożliwia generowanie raportów (raportowanie na podstawie baz danych) z systemu VMS. Każdy raport w systemie jest zadaniem, każdy posiada własne uprawnienia. Użytkownik może posiadać dostęp do określonego zadania raportu, jeśli posiada odpowiednie uprawnienia.
- Platforma udostępnia następujące typy raportów:
    - Raport alarmów
    - Raporty dla wideo (dotyczące zapisu, zakładek, detekcji ruchu i inne)
    - Zachowania stanu sprawności i raporty o statystykach kondycji systemu
- Raporty ogólne, własne i szablony raportów

- Użytkownik może utworzyć raport ogólny z dostępnej listy, wybrać stworzony szablon raportu lub utworzyć nowy raport albo szablon raportu.

### 2.14. Integracja z Microsoft Active Directory

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

### 2.15. Bezpieczeństwo Użytkowników i Zarządzanie Uprawnieniami

- Platforma VMS umożliwia konfigurację i zarządzanie użytkownikami i grupami użytkowników. Użytkownik może dodawać, usuwać lub zmieniać użytkownika lub grupę użytkowników, jeśli posiada do tego odpowiednie uprawnienia.
- Prawa dostępu i uprawnienia dzielone przez wielu użytkowników są określane jako Grupy Użytkowników. Członkowie grupy posiadają te same prawa, co ich grupa nadrzędna. Dozwolone jest dodawanie podgrup.

### 2.16. Raporty Incydentów

- Raporty incydentów umożliwiają operatorom systemu tworzenie raportów zdarzeń, które wystąpiły podczas ich zmiany. Dostępne są zarówno zdarzenia związane z wideo.
- Operator może utworzyć niezależny raport o zdarzeniu lub powiązać go z alarmami.

### 2.17. Integracja kamer i urządzeń do oprogramowania platformy VMS

- VMS musi być oparty na strukturze otwartej, która umożliwia wykorzystanie będących w powszechnej dystrybucji stacji klienckich, serwerów urządzeń infrastruktury sieci oraz pamięci masowych.
- VMS musi oferować pełne i skalowalne oprogramowanie nadzoru wideo, które umożliwia dodawanie kamer.
- VMS musi obsługiwać enkodery wideo (wideoserwery) przetwarzające analogowe sygnały wideo na strumienie cyfrowe oraz kamery IP, nazywanymi cyfrowymi źródłami video. VMS musi współpracować z enkoderami i kamerami IP wielu producentów.
- Wszystkie strumienie wideo z kamer analogowych lub kamer IP muszą być kodowane cyfrowo w jednym ze standardów kompresji MPEG-4, MPEG-2, MJPEG, H.264, H.265.
- Wszystkie pliki audio z serwerów wideo IP muszą być kodowane cyfrowo jako g711 (u-law), g721, g723 lub AAC i jednocześnie nagrywane w czasie rzeczywistym.

Oprogramowanie do rejestracji i zarządzania wideo ma być zintegrowane z różnymi kamerami IP (w tym kamery kopułkowe, stało pozycyjne i PTZ) i klawiaturami PTZ IP w tym co najmniej z urządzeniami następujących producentów:

- Acti
- ArecontVision
- Axis
- Bosch
- Ganz
- IQinvision
- JVC
- Mobotix
- Panasonic
- Pelco
- Samsung
- Sanyo
- Sony
- UDP

- Verint
- Vivotek

Zastosowane w systemie kamery muszą znajdować się na liście wspieranych urządzeń publikowanej przez producenta oprogramowania platformy VMS, bez żadnych ograniczeń formalnych i technicznych.

Integracja z ww. kamerami ma być realizowana poprzez natywne oprogramowanie układowe, dostarczający unikalny zestaw narzędzi dla danego urządzenia niezbędny do uzyskania pełnej funkcjonalności dostępnej w urządzeniu. Dodatkowo oprogramowanie do rejestracji i zarządzania wideo ma umożliwiać obsługę kamer IP wspierających protokół ONVIF Profile S. Oprogramowanie do rejestracji i zarządzania wideo ma umożliwiać obsługę wideo ze wszystkich kamer w systemie z rozdzielczością, poklatkowością, rodzajem kompresji oraz jakością kompresji zgodną z wymaganiami określonymi dla stosowanych kamer.

**Kamery analogowe PTZ mają zostać dołączone do cyfrowej platformy VMS poprzez zastosowanie enkoderów kompatybilnych z platformą VMS.**

Panel Konfiguracji musi umożliwiać tworzenie harmonogramów, do których można dołączyć dowolną funkcjonalność z poniższych:

- Jakość wideo (dla każdego strumienia wideo każdej kamery)
- Nagrywanie (dla każdej kamery)
- Jasność, Kontrast, Nasycenie (dla każdej kamery)
- Wykrycie ruchu (dla każdej strefy wykrywania kamery)
- Wykonanie sekwencji kamery
- Panel Konfiguracji umożliwia tworzenie nieograniczonej liczby harmonogramów nagrywania i przypisuje dowolną kamerę do harmonogramu.
- Panel Konfiguracji umożliwia ustawianie protokołu PTZ dla dowolnego portu szeregowego enkodera i pozwala na stosowanie kamer różnych producentów w jednym systemie.

### 2.18. Rejestrowanie

- Rola Rejestratora wideo wykorzystuje bazę danych zdarzeń i stempli czasowych w celu zaawansowanego wyszukiwania audio/wideo.
- Rejestrator zabezpiecza zarchiwizowane pliki audio/wideo i bazę danych systemu przed dostępem sieciowym użytkownika bez praw administratora.
- Rejestrator cyfrowo podpisuje zapisane wideo za pomocą kryptograficznego, 124-bitowego klucza RSA typu publiczny/prywatny.
- Rejestrator wykrywa enkodery i kamery IP w innych segmentach sieci, łącznie z Internetem oraz w sieciach używających (lub nie) translacji adresu sieciowego (NAT).
- Rejestrator może konfigurować odstęp klatek kluczowych (I-frame) w sekundach lub w liczbie klatek.
- Rejestrator posiada opcję nagrywania przed lub po alarmie, która może być ustawiona od 1 sekundy do 3 minut dla każdej kamery oddzielnie.
- Rejestrator posiada opcję przechowywania plików wideo i audio na podstawie zdarzeń takich jak wykrycie ruchu i makra
- Rejestrator wykrywa ruch wideo dla każdej kamery osobno, zgodnie z siatką wykrywania ruchu składającą z ponad 1200 bloków wykrywających ruch. Wszystkie ustawienia wykrywania ruchu wideo są konfigurowalne zgodnie ze harmonogramem. Ogólny próg wykrywalności umożliwia zmniejszenie czułości wykrywania ruchu tam, gdzie sygnał wideo jest zakłócony lub tam, gdzie występuje wiele błędnych trafień.
- Rejestrator udostępnia wiele harmonogramów nagrywania, które mogą być przypisane do pojedynczej kamery, każdy harmonogram może być utworzony w oparciu o następujące parametry:
    - Tryb nagrywania:
        - Ciągły
        - Podczas ruchu/Ręczny
        - Ręczny
        - Wyłączony

- Wzór powtarzania
  - Raz w wybrane dni
  - Wybrane dni w roku
  - Wybrane dni w miesiącu
  - Wybrane dni w tygodniu
  - Codziennie
- Czas nagrywania
  - Cały dzień
  - Wybrane przedziały czasu
  - W dzień lub w nocy zgodnie z czasem wschodu i zachodu słońca, obliczanego automatycznie zgodnie z porą roku i lokalizacją geograficzną.

- Rejestrator umożliwia kodowanie każdej kamery (źródła wideo) wielokrotnie w tym samym lub różnych formatach wideo MPEG-4, MPEG-2, MJPEG, H.264, H.265 co ograniczone jest jedynie przez możliwości każdego ze źródeł strumienia IP (enkoder, kamera IP). Gdy dostępne jest wiele strumieni wideo z tej samej kamery, użytkownicy mogą wybrać dowolny z nich zgodnie z przypisaną im funkcją.
- Rejestrator zezwala na różną jakość wideo, zgodnie z określonym harmonogramem. Schematy te posiadają tę samą możliwość konfiguracji, jak harmonogramy nagrywania Jakość wideo oparta jest, ale nie ograniczona do następujących parametrów:
  - Maksymalna przepływność (bit rate)
  - Maksymalna poklatkowość (framerate)
  - Jakość obrazu
  - Odstęp klatek kluczowych
- Rejestrator może komunikować się z cyfrowym źródłem video (enkoder, kamera IP) za pomocą 128 bitowego kodowania SSL.
- Rejestrator może komunikować się z cyfrowym źródłem video (enkoder, kamera IP) za pomocą bezpiecznego protokołu HTTPS.
- Rejestrator może odbierać wiele transmisji multicast UDP bezpośrednio z cyfrowego źródła video (enkoder, kamera IP)
- Rejestrator ma możliwość przekierować strumienie audio/wideo do oglądających je klientów w sieci obsługującej multicast UDP tam, gdzie konfiguracja sieci ogranicza cyfrowe źródło video przed przesyłem multicastowych strumieni UDP.
- Rejestrator może przekierować strumienie audio/wideo do aktywnie oglądających je klientów w sieci za pomocą protokołu unicast UDP lub TCP.
- Rejestrator umożliwia administratorowi wybór dysków wykorzystywanych do archiwizacji i ustawiania limitu objętości dla każdego z nich.
- Rejestrator umożliwia administratorowi archiwizowanie różnych kamer w różnych grupach dysków
- Rejestrator oferuje następujące opcje kasowania archiwum, osobno dla każdej kamery:
  - Po upływie określonej liczby dni
  - Kasowanie najstarszych plików, kiedy dysk się zapełni
  - Zatrzymanie archiwizowania, kiedy dysk jest pełny
- Rejestrator umożliwia chronienie ważnych sekwencji wideo przed kasowaniem.
  - Do wyznaczonej daty
  - Przez określoną liczbę dni
  - W nieskończoność (aż do usunięcia ochrony)
- Rejestrator umożliwia administratorowi określenie ilości miejsca na dysku, które jest zajęte przez chronione wideo.
- Rejestrator może zmniejszać wielkość obrazów wideo w celu oszczędzania miejsca na dysku. Możliwe jest zmniejszenie wielkości strumienia poprzez zmniejszanie ilości klatek kluczowych w kompresjach H.264, MPEG-4, MJPEG.
- Rejestrator obsługuje możliwość nagrywania materiału wideo w pamięci podręcznej kamery (karta SD) i oferując następujące funkcje:
  - Odtwarzanie w różnych prędkościach wideo zapisanego w urządzeniu cyfrowym źródłem video (enkoder, kamera IP)

- Możliwość transferu (kopiowania z usunięciem) wideo zapisanego cyfrowym źródle video (enkoder, kamera IP) do Rejestratora zgodnie z harmonogramem, zdarzeniem lub ręcznie.
- Możliwe jest filtrowanie transferowanego wideo za pomocą jednego lub wielu filtrów, np.:
  - Przedziału czasu,
  - Zdarzenia z analityki wideo,
  - Żądania odtwarzania,
  - Alarmów

- Rejestrator powinien umożliwiać ograniczenie strumienia wideo w celu oszczędzenia pamięci, przy czym opcje ograniczenie to realizowane jest poprzez następujące opcje:
  - strumień H.264 ograniczenie do: wszystkie klatki kluczowe, 1fps, 2 sec/klatke, 5 sec./klatke, 10 sec./klatke, 15 sec./klatke, 30 sec./klatke, 60 sec./klatke, 120 sec./klatke
  - strumień MPEG-4 ograniczenie do: wszystkie klatki kluczowe, 1fps, 2 sec/klatke, 5 sec./klatke, 10 sec./klatke, 15 sec./klatke, 30 sec./klatke, 60 sec./klatke, 120 sec./klatke
  - strumień MJPEG ogranicznie do: 15 fps, 10 fps, 5 fps, 2 fps, 1 fps, 2 sec/klatke, 5 sec./klatke, 10 sec./klatke, 15 sec./klatke, 30 sec./klatke, 60 sec./klatke, 120 sec./klatke

### 2.19. Przesyłanie strumieni Wideo

- W platformie bezpieczeństwa VMS występuje oddzielna rola/mechanizm odpowiedzialna za routowanie wideo i audio w sieci lokalnej i rozległej ze źródła cyfrowego (enkoder, kamera IP) do celu (np. aplikacji klienckiej).
- Mechanizm ten współpracuje z wieloma protokołami przesyłu, takimi jak unicast TCP, unicast UDP oraz multicast UDP. Współpracuje z IGMP (Internet Group Management Protocol) aby ustalić przynależność grup multicastowych.
- Możliwa jest konwersja przekaz z dowolnego obsługiwanego protokołu przekazu, tj.:
  - Multicast UDP do Unicast TCP
  - Multicast UDP do Unicast UDP
  - Unicast TCP do Multicast UDP
  - Unicast UDP do Multicast UDP
- Kiedy używamy strumienia Multicast z kamery, VMS musi zezwolić na przesłanie strumienia "na żywo" bezpośrednio z kamery do aplikacji klienckiej, omijając przy tym transfer do rejestratora.

### 2.20. Możliwości transferowe archiwum wideo

- Transfer archiwum powinien zapewnić możliwość do:
  - przesłania nagrania wideo z serwera do innego serwera w tym samym czasie
  - przesłania nagrania wideo z systemu sfederowanego do innego serwera
  - przesłania nagrania wideo z karty pamięci umieszczonej w kamerze do serwera
- Platforma musi umożliwić transfer nagrania wideo po wcześniej zaprogramowanym harmonogramie lub poprzez ręczne zaznaczenie przy połączeniu
- Platforma musi umożliwić filtrowanie nagrania oraz transferowanie tylko zdefiniowanych fragmentów, przy czym definiowanie powinno odbywać się po poniższych filtrach:
  - Całe archiwum w przypadku utraty wizji z kamery
  - Alarmy
  - Odtwarzanie nagrania z karty pamięci
  - Zdarzenia wyzwolone poprzez analitykę obrazu
  - Detekcje ruchu
  - Zakładki
  - Wyzwolenie wejścia
  - Przedział czasowy
- Platforma musi posiadać interfejs graficzny umożliwiający wyświetlenie transferowanych nagrań z archiwum. Interfejs powinien wyświetlać obecne, zdefiniowane oraz zaplanowane żądanie transmisji wideo. Platforma musi również posiadać możliwość edytowania, wyzwalania oraz anulowania transferu nagrania poprzez interfejs.

### 2.21. Wykorzystanie Analityki

Platforma musi być natywnie kompatybilna z co najmniej 10 producentami analityki wideo. Dodanie zaawansowanej analityki wykrywania zdarzeń oraz narzędzi analitycznych do VMS musi być zapewniona poprzez szereg możliwości analitycznych wbudowanych w wielu najnowszych kamerach IP, jak również u wielu specjalizujących się producentów zaawansowanej analityki wideo.