ZAŁĄCZNIK NR 1

OPIS PRZEDMIOTU ZAMÓWIENIA – PROGRAM FUNKCJONALNO-UŻYTKOWY

Dotyczy: „Wykonanie dokumentacji projektowej modernizacji systemu monitoringu terenu Miasteczka Akademickiego UMCS."

Zamawiający: Uniwersytet Marii Curie-Skłodowskiej w Lublinie, 20-031 Lublin Pl. Marii Curie Skłodowskiej 5.

Osoby prowadzące:

- **mgr inż. Adam Kargul**– branża elektryczna tel. 81 537-53-10

Opis przedmiotu zamówienia.

Przedmiotem zamówienia jest: **„Wykonanie dokumentacji projektowej modernizacji systemu monitoringu terenu Miasteczka Akademickiego UMCS."**

Zakres zamówienia obejmuje:

1) wykonanie inwentaryzacji istniejącej zabudowy nieruchomości w zakresie objętym przedmiotem zamówienia, niezbędnym do sporządzenia dokumentacji projektowej i kosztorysów;
2) wykonanie dokumentacji projektowej będącej przedmiotem umowy zgodnie z Rozporządzeniem Ministra Rozwoju i Technologii z dnia 20 grudnia 2021r. w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno - użytkowego (Dz. U. Nr 2021 poz. 2454);
3) pełnienie nadzoru autorskiego zgodnie z przepisami prawa budowlanego na każde wezwanie telefoniczne Zamawiającego, nie później niż trzeciego dnia, licząc od dnia powiadomienia;
4) sporządzenie kosztorysu inwestorskiego dla wszystkich branż na podstawie rozporządzenia Ministra Rozwoju i Technologii z dnia 20 grudnia 2021r. (Dz. U. z 2021., poz. 2458) w sprawie określenia metod i podstaw sporządzania kosztorysu inwestorskiego, obliczania planowanych kosztów prac projektowych oraz planowanych kosztów robót budowlanych określonych w opisie przedmiotu zamówienia (programie funkcjonalno-użytkowym);
5) sporządzenie szczegółowych specyfikacji technicznych wykonania i odbioru robót dla wszystkich branż objętych zakresem opracowania;
6) udzielanie odpowiedzi w terminie 2 dni na pytania w postępowaniach przetargowych dotyczących robót budowlanych realizowanych na podstawie wykonanej dokumentacji projektowej;
7) wykonanie przedmiotu umowy z należytą starannością i zgodnie z zasadami wiedzy technicznej, obowiązującymi w tym zakresie przepisami szczegółowymi oraz normami, aprobatami, specyfikacjami technicznymi i systemami odniesienia;
8) bieżąca współpraca z Zamawiającym i dokonywanie uzgodnień z jego przedstawicielami i Użytkownikiem;
9) każdorazowe uzgadnianie z Zamawiającym treści i zakresu informacji związanych z przedmiotem umowy w przypadku zamiaru ich wykorzystania do celów reklamowych i statystycznych;
10) uzyskanie niezbędnych do celów projektowych warunków, uzgodnień rzeczoznawców, zgód i/lub opinii, sprawdzeń rozwiązań projektowych w zakresie wynikającym z przepisów, o ile zachodzi taka potrzeba;
11) wyjaśnianie wątpliwości dotyczących projektu i zawartych w nim rozwiązań;
12) w przypadku wystąpienia kolizji projektowanego okablowania sieci monitoringu z istniejącą infrastrukturą techniczną znajdującą się w obrębie objętym projektowaniem należy uzyskać niezbędne uzgodnienia w zakresie rozwiązań usunięcia kolizji ze wszystkimi właścicielami (lub zarządcami) tej infrastruktury.
12) zaopatrzenie dokumentacji projektowej lub jej części w wykaz opracowań oraz pisemne oświadczenie, że dostarczona dokumentacja obiektu budowlanego jest wykonana zgodnie z umową, obowiązującymi przepisami i normami i że została wydana w stanie zupełnym (kompletna z punktu widzenia celu, któremu ma służyć);
13) przygotowanie opracowań stanowiących przedmiot umowy przez osoby posiadające uprawnienia budowlane do projektowania bez ograniczeń w odpowiedniej specjalności;
16) nieodpłatne wykonanie aktualizacji kosztorysów inwestorskich w sytuacji przesunięcia terminów wykonania robót budowlanych na podstawie wykonanej dokumentacji projektowej w terminach uzgodnionych z Zamawiającym;
17) sporządzenie dokumentacji w taki sposób by uwzględniała ona opis wykonania robót ze szczególną starannością przy uwzględnieniu przepisów bhp, ze względu na realizację robót budowlanych przy obiekcie;
18) przedmiotu zamówienia zawartego w dokumentacji projektowej nie można opisywać przez wskazanie znaków towarowych, patentów lub pochodzenia chyba, że jest to uzasadnione specyfiką przedmiotu i Wykonawca nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń, a wskazaniu takiemu towarzyszą wyrazy „lub równoważny". W takim przypadku, Wykonawca, który powołuje się na rozwiązanie równoważne, przygotowując dokumentację projektową musi wykazać, w jaki sposób należy określić równoważność;
19) Uzyskanie decyzji zatwierdzającej projekt i udzielającej pozwolenie na budowę z Wydziału Architektury i Budownictwa Urzędu Miasta Lublina (o ile jest wymagane);
20) Zgłoszenie w Wydziale Architektury i Budownictwa Urzędu Miasta Lublin robót nie wymagających pozwolenia na budowę; (o ile jest wymagane).

Zakres szczegółowy przedmiotu zamówienia:

1) Sporządzenie kompletnej dokumentacji projektowej budowlanej i technicznej
2) Sporządzenie szczegółowej specyfikacji wykonania i odbioru robót budowlanych.
3) Sporządzenie kosztorysu inwestorskiego.
4) Sporządzenie przedmiaru robót.

Niezbędne dane dotyczące przestrzeni monitorowanej

System monitoringu ma za zadanie wspomagać pracę policji oraz innych służb odpowiedzialnych za utrzymanie porządku i ładu publicznego. System będzie służył do obserwacji osób, pojazdów oraz innych elementów zlokalizowanych w monitorowanej przestrzeni. Obserwacji będą podlegać zdarzenia takie jak np. niszczenie własności prywatnej i publicznej, śmiecenie, napad lub włamanie, niedozwolony handel, bójki, zaczepki pieszych, wykroczenia drogowe, wypadki, przestępstwa samochodowe, zabronione zachowania społeczne (w tym m. in. wandalizm, picie alkoholu) oraz natężenie ruchu, liczba wolnych miejsc parkingowych i inne służące sporządzaniu danych statystycznych.

Przestrzenią stanowiącą zakres opracowania jest teren w obrębie: linia Domy Studenta Amor-Babilon, skarpa stanowiąca granicę Parku Akademickiego, budynek Centrum Analityczno-Programowe Ecotech-Complex, ulica Langiewicza.

Wymagania szczegółowe dotyczące urządzeń i parametrów technicznych systemu monitoringu.

Projektowane kamery zewnętrzne dla systemu monitoringu muszą charakteryzować się następującymi cechami:

Obraz:

- Przetwornik CMOS nie mniejszy niż 1 /2.7”
- Ilość efektywnych pikseli przetwornika większa niż 5 Megapikseli.
- Powierzchnia piksela na przetworniku nie mniejsza niż 4 um2.
- Światłoczułość przetwornika powinna wynosić przynajmniej 12,000e-/Lux·sec.
- Kamera wyposażona w obiektyw zapewniający kąty widzenia (horyzontalne) w zakresie >100˚ do <35˚ (najszerszy kąt może być większy. Dopuszcza się większy zakres – mniejszy kąt po przybliżeniu). Obiektyw musi posiadać funkcję zdalnego ustawiania ogniskowej i ostrości.
- Obiektyw o jasności przynajmniej F1.6 dla początku ogniskowej. Obiektyw musi posiadać sterowanie przysłoną wykorzystującą P-Iris.
- Możliwość przesyłania video z prędkością 30 ramek na sekundę w rozdzielczości 2650 x 1920 lub większej.
- Obsługa przynajmniej 3 strumieniu obrazu, z czego przynajmniej dwa muszą obsługiwać rozdzielczość 2650 x 1920 i prędkości 20 ramek na sekundę.
- Procesor obrazu musi posiadać wystarczającą moc obliczeniową do wygenerowania przynajmniej 3 strumieni w rozdzielczości FullHD, z czego jeden w 60 ramek na sekundę, a pozostałych w pełnych 30 ramkach na sekundę.
- Kamera musi być wyposażona w przetwornik Multi Exposure HDR o mocy przynajmniej 120 dB. Nie dopuszcza się samej technologii WDR.
- 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 posiadać możliwość wygenerowania strumienia FullHD w MJPEG z prędkością przynajmniej 30 ramek na sekundę.
- Promiennik podczerwieni z minimalnym zasięgiem 40m, pracujący w zakresie 850nm lub 920nm.
- Przetwornik kamery musi posiadać QE przynajmniej 60% dla zakresu podczerwieni wykorzystywanego w zamontowanych diodach.

Procesor kamery:

- Kamera musi posiadać procesor wyposażony w przynajmniej 4 rdzenie, taktowane 1Ghz.
- Procesor kamery musi umożliwiać obsłużenie następujących analityk obrazu bezpośrednio na kamerze:
    - Detekcja porzuconego obiektu
    - Detekcja intruza w strefie
    - Detekcja sabotażu obrazu kamery
    - Niewłaściwy kierunek poruszania w strefie
    - Detekcja podejrzanego wałęsania się
    - Liczenie obiektów
    - Detekcja usunięcia obiektu
    - Detekcja zatrzymanego pojazdu

Interfejsy i integracja:

- Kamera musi posiadać wejście i wyjście AUDIO. Rejestracja i przesyłanie dźwięku musi odbywać się z wykorzystaniem kodowania AAC lub MP3.

• W przypadku wystąpienia alarmu na kamerze (analiza obrazu, zanik sieci, sabotaż kamery, zdarzenie cykliczne, naruszenie wejścia alarmowego w kamerze), kamera musi posiadać możliwość wysłania komendy CGI na wybrany adres sieciowy.

• Kamera musi posiadać przynajmniej 2 wejścia alarmowe oraz 1 wyjście. Dopuszcza się stosowanie zewnętrznych modułów rozszerzających, jeśli będą dostarczone, zamontowane i skonfigurowane razem z kamerami.

• Kamera musi posiadać certyfikację ONVIF zapewniająca kompatybilność z innymi urządzeniami.

• Kamera musi wspierać następujące profile standardu ONVIF: S, G, T, Q.

• Obudowa kamery musi posiadać szczelność minimalnie IP66, oraz odporność na uderzenia na poziomie IK10.

• Kamera musi posiadać możliwość pracy przy szerokim zakresie temperatur, przynajmniej -40 do +50. Dopuszcza się stosowanie zewnętrznych grzałek, o ile będą automatycznie uruchamiane w przypadku spadku temperatury, oraz zasilane będą z tego samego źródła co kamera.

• Kamera musi umożliwiać zasilenie z różnych źródeł PoE +, 12VDC lub 24AC. Zasilanie musi umożliwiać redundancje – w przypadku zaniku jednego ze źródeł, kamera powinna automatycznie bez restartu przełączyć się na zapasowe źródło.

- Kamera musi występować na liście wpieranych urządzeń Genetec.
- Kamera musi posiadać akcesoria do montażu na ścianie jak i na słupie.

<u>Wymagania ogólno-funkcjonalne do systemu zarzadzania wideo (VMS).</u>

Parametry minimalne i wymagania funkcjonalne dla systemu zarządzania bezpieczeństwem

1) Oferowany system musi spajać w sposób logiczny i przez wspólny interfejs użytkownika co najmniej 4 własne moduły: zarządzanie źródłami video, kontrola dostępu, rozpoznawania tablic rejestracyjnych, rozpoznawanie twarzy.
2) 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.
3) 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.
4) 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.
5) 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.
6) 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.
7) Otwartość systemu musi umożliwiać wykorzystanie będących w powszechnej dystrybucji stacji klienckich, serwerów urządzeń infrastruktury sieci oraz pamięci masowych.
8) System musi posiadać możliwość dekodowania strumieni H.264 oraz H.265 po stronie karty graficznej, z możliwością przydzielenia dedykowanych kart do poszczególnych kodeków.
9) System musi obsługiwać kodeki MJPEG, MPEG4, H.264, H.265, MxPEG.
10) 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.
11) 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, 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.
12) 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, Paxton, NEDAP. 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, 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.

13) 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
14) 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, 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.
15) 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.
16) 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.
17) 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 aplikacja serwerową i powinna być dostępna dla wszystkich kanałów dostępnych dla danej licencji.
18) 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).
19) 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.
20) 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.
21) System VMS musi umożliwiać tworzenie interaktywnych przycisków umożliwiających wywoływanie komend CGI, wysyłanie żądań http, resetowanie liczników, generowanie alarmów, uzbrajanie/rozbrajanie systemów alarmowych, wyzwalanie 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.
22) Licencja na system VMS nie powinna być przypisana do specyfikacji sprzętowej serwera i umożliwiać przenoszenie na inne serwery bez ingerencji producenta.
23) System musi umożliwiać podłączenie 250 klientów (android, iOS, aplikacja kliencka, przeglądarka) w tym samym momencie. Jeśli taka funkcjonalność wymaga dodatkowej licencji, powinna być ona dostarczona wraz z systemem.
24) 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.
25) 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.

26) VMS będzie działał na standardowych systemach operacyjnych Windows i różnych mobilnych systemach operacyjnych dla platform opartych na aplikacjach mobilnych.
27) VMS musi obsługiwać funkcję multicastu, a także możliwość unicastu dla każdego urządzenia peryferyjnego kamery w wielu instancjach jednocześnie.
28) Producent systemu VMS musi umożliwiać świadczenie wsparcia (aktualizacji, poprawek) dla systemu na okres minimum 10 lat.

Funkcja federacja dla obsługi zdalnych systemów:

1) 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.
2) 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.
3) 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.
4) Funkcja federacji musi unifikować wiele odrębnych (logicznie, lub geograficznie) systemów bezpieczeństwa.
5) Federacja musi obsługiwać alarmy i kamery.
6) System musi umożliwiać nagrywanie dowolnego ekranów innych stacji klienckich i serwerów wraz z obsługa nagrywania ściany wizyjnej.

Integracja z Microsoft Active Directory

1) 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.
2) Jeśli się zezwoli, 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 VMS.

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

1) System musi obsługiwać własne opcje pracy w przypadku wystąpienia awarii (failover).
2) 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 standbay 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 standbay musi obywać się kaskadowo. Jeśli taka funkcjonalność wymaga dodatkowej licencji, powinna być ona dostarczona wraz z systemem.
3) Zapasowy serwer centralny powinien mieć możliwość zachowania bazy danych konfiguracji zsynchronizowanej z głównym serwerem centralnym.
4) System VMS musi umożliwiać tworzenie oddzielnych baz danych dla zdarzeń, użytkowników, nagrań oraz dla audytu systemu wraz z oddzielnym sposobem szyfrowania.
5) System musi automatycznie szyfrować wszystkie bazy danych (również bazę nagrań), jak również dodatkowo zabezpieczać je hasłem.
6) 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)
7) VMS musi wykorzystywać czasowe tokeny do zestawiania połączeń sieciowych, aby zabezpieczyć system przed atakami DoS.
8) System musi umożliwiać tworzenie własnych polityk haseł użytkowników, definiujących długość hasła, ilość prób logowania, ilość znaków specjalnych.
9) 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.
10) System musi dokumentować wszystkie zmiany związane z użytkownikiem w aplikacji i podłączonych urządzeniach peryferyjnych ze środowiskiem aplikacji.

Aplikacja Kliencka

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

2) 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.
3) 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.
4) Aplikacja kliencka musi być dostępna w języku polskim.
5) Aplikacja kliencka musi mieć możliwość zablokowania powłoki Windows, aby uniemożliwić zamknięcie czy zminimalizowanie aplikacji bez podania hasła nadanego przez administratora.
6) 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).
7) Aplikacja kliencka musi posiadać interfejs do eksportowania nagrań z 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).
8) Aplikacja kliencka musi mieć możliwość odtwarzania materiały z przyśpieszeniem 128x oraz spowolnieniem 128x.
9) System będzie w stanie pobierać nagrane wideo na podstawie kryteriów wyszukiwania użytkowników, w tym kombinacji:
    a. identyfikator referencyjny kamery,
    b. data i godzina nagrania z kamery,
    c. zaznaczenie obszaru wokół interesującego obiektu w celu ustalenia, kiedy obiekt pojawił się w scenie,
    d. zdarzenia alarmowe,
10) zakładki dodawane automatycznie lub ręcznie przez użytkownika,
11) alfanumeryczny ciąg metadanych (np. numer transakcji nagrany za pomocą wideo z innych systemów, numery tablic rejestracyjnych, kody kreskowe, dane z wag itp.).
12) 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.
13) VMS musi posiadać funkcjonalność rozmywania ruchu na eksportowanym materiale wideo. Jeśli funkcjonalność wymaga dodatkowej licencji powinna być ona dostarczona wraz z systemem.
14) Aplikacja musi oferować interfejs do wyszukiwania ciągów znaków odbieranych i filtrowanych przez sniffer po stronie serwera.
15) 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.
16) 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

1) System musi posiadać zintegrowane narzędzie do edycji i tworzenia map rozmieszczenia elementów technicznego systemu zabezpieczeń. Graficzny interfejs mapy musi spełniać co najmniej następujące wymagania:
2) Wyświetlanie wielu map dla jednego oraz dla wielu obszarów
3) Wyświetlanie map jako warstw
4) 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.
5) Wyświetlanie podkładów mapowych w postaci bitmap
6) Przełączanie się pomiędzy mapami poprzez aktywne przyciski, również między mapami GIS i bitmapami
7) Wyświetlanie na mapie aktywnych ikon urządzeń w systemie,
8) Wyświetlanie na mapie aktywnych obszarów obserwacji kamer stacjonarnych w systemie
9) 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.
10) Centralne zarządzanie mapami.

Otwarta architektura

1) System musi być neutralny w stosunku do producentów urządzeń technicznych systemów bezpieczeństwa dostępnych na rynku i umożliwiać ich integracje udostępniając Software Development Kits (SDK), Driver Development Kits (DDK), Web Service SDK.
2) System musi posiadać możliwość dodania pluginów integrujących systemy zewnętrzne, takie jak:
    a. Analityka wideo
    b. Zewnętrzne systemy firm trzecich
3) 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.

Wymagania ogólne dotyczące formy prac projektowych.

1. Wykonawca uzgodni pisemnie z Zamawiającym przyjęte rozwiązania funkcjonalno-użytkowe.
2. Projekt budowlany i techniczny (wszystkich branż), przedmiary, kosztorysy inwestorskie oraz specyfikacje techniczne, które będą podstawą do przeprowadzenia procedury przetargowej.
3. Dokumentacja ma być wykonana zgodnie z obowiązującymi przepisami.
4. Wykonawca zobowiązany jest do pełnienia nadzoru autorskiego nad realizacją robót remontowych zgodnie z przedstawionym opracowaniem.
5. Prace projektowe należy wykonać zgodnie z obowiązującymi normami i przepisami prawa, w tym w szczególności:
   1) Ustawą z dnia 7 lipca 1994 r. Prawo budowlane (Dz. U. z 2023r. poz. 682).
   2) Rozporządzeniem Ministra Infrastruktury z dnia 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz. U. 2022r. poz. 1225).
   3) Ustawą z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz. U. 2019r. poz. 1372 ze zm.).
   4) Ustawą z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (Dz. U. 2022 poz. 503 tekst jednolity);
   5) Rozporządzeniem Ministra Pracy i Polityki Socjalnej z 26 września 1997r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy (Dz. U. 2003 Nr 169 poz.1650 ze zm.).
   6) Rozporządzeniem Ministra Infrastruktury z dnia 6 lutego 2003 r. w sprawie bezpieczeństwa i higieny pracy podczas wykonywania robót budowlanych (Dz. U. 2003 Nr 47 poz. 401 ze zm.).
   7) Ustawą z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów oraz inżynierów budownictwa (Dz. U. 2023r. poz. 551 ze zm.).
   8) Ustawą z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2022r. poz. 1710 t.j.).
   9) Rozporządzenie Ministra Rozwoju i Technologii z dnia 20 grudnia 2021 r. w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego (Dz. U. z 2021r. poz. 2454.).
   10) Rozporządzenie Ministra Rozwoju i Technologii z dnia 20 grudnia 2021 r. w sprawie określenia metod i podstaw sporządzania kosztorysu inwestorskiego, obliczania planowanych kosztów prac projektowych oraz planowanych kosztów robót budowlanych określonych w programie funkcjonalno-użytkowym (Dz. U. 2021 Nr 130 poz. 2458).
   11) Inne przedmiotowe obowiązujące.
6. Dokumentację należy przekazać Inwestorowi w wersji papierowej oraz elektronicznej w ilościach ujętych poniżej:
   1) inwentaryzacja niezbędna do celów projektowych w wersji papierowej – 2 egz.,
   2) projekt budowlany (dotyczy wszystkich branż w tym projektów technicznych, planu zagospodarowania terenu oraz projektu architektoniczno-budowlanego) – 4 egz. w tym 3 oryginały projektu budowlanego i 1 kopia oryginału projektu budowlanego;
   3) projekt techniczny (dotyczy wszystkich branż) – 4 egz. w tym 4 oryginały projektu wykonawczego;
   4) kosztorysy inwestorskie oraz przedmiary robót w wersji papierowej – po 2 egz.,
   5) specyfikacja techniczna wykonania i odbioru robót w wersji papierowej – 2 egz.,
   6) inwentaryzacja, dokumentacja projektowa budowlana i techniczna w wersji elektronicznej – 2 egz. (część opisowa powinna być dostarczona w formacie *.doc., schematy, plany, rysunki winny być dostarczone w standardzie plików PDF i *.dwg.,
   7) w przypadku zastosowania innego formatu plików (umożliwiającego edycję) należy dostarczyć odpowiednie oprogramowanie wraz z licencją,
   8) kosztorysy inwestorskie oraz przedmiary robót w wersji elektronicznej *.ath (Norma Pro) – po 2 egz.,
   9) specyfikacja techniczna wykonania i odbioru robót w wersji elektronicznej (format edytowalny *.doc) – 2 egz.

Zaleca się, aby Wykonawca dokonał wizji lokalnej w miejscu opisanym w przedmiocie zamówienia oraz uzyskał na swoją odpowiedzialność i ryzyko wszelkie istotne informacje, które mogą być przydatne do przygotowania oferty. Wizja lokalna winna być wykonana na koszt własny Wykonawcy.

Wszystkie rozwiązania dotyczące zakresu opracowania jak i wyposażenia musza zostać skonsultowane z Zamawiającym, w celu weryfikacji najlepszego rozwiązania.

Opracowała:
mgr inż. Adam Kargul