Załącznik Nr 1A do SWZ

Opis przedmiotu zamówienia

Dostawa i montaż systemu kontroli dostępu do obiektu

- Dostawa i montaż 3 kompletów szlabanów wjazdowych i wyjazdowych po 4 m każdy (6 szlabanów) ,
- Dostawa i montaż kamer 3 LPR (rozpoznawanie tablic rej), systemu otwierania opartego także o aplikacja telefoniczne , otwarcie awaryjne,
- Wykonanie brukowania w rejonie szlabanów w celu montażu tzw. pętli indukcyjnych (wjazd i wyjazd),
- Wykonanie montażu samozamykaczy dla bramki wejściowej w miejscu uzgodnionym z Zamawiającym ,
- Wykonanie systemu KD oraz montaż trzymacza dla bramki wejściowej,
- Zakup bram 3 sztuki po 2 skrzydła wraz z zachowaniem symbolu,
- Dostawa licencji wraz z oprogramowaniem dla systemu LPR i systemu KD,
- Dostawa i montaż 5 czytników dla systemu KD,
- Dostawa i montaż 4 kamer nadzorujących bramy,
- Dostawa i montaż kontrolerów do systemu aplikacji mobilnej dla 3 szlabanów i 4 bram
- Dostawa i montaż siłowników do 4 bram;
- Dostawa i montaż systemu radiowego (pilot) dla bramy głównej, kompatybilny z istniejącym systemem,
- Dostawa i montaż stanowiska zarządzającego system LPR i KD,
- Dostawa i montaż domofonu PoE (IP) -3 kpl oraz 3 jednostki odbiorcze.

Opis działania :

Bramy stalowe będą otwierane zgodnie z harmonogramem skonfigurowanym w systemie kontroli dostępu za pomocą siłowników .Szlabany wjazdowe na parkingi otwierane przez kierowca za pomocą aplikacji która będzie zarządzana przez inwestora (np. dział IT), czytnika KD lub za pomocą rozpoznania tablicy rejestracyjnej pojazdu (wcześniej wpisana do bazy).

W przypadku pojazdów uprzywilejowanych (otwarcie nastąpi za pomocą detekcji sygnału dźwiękowego. Awaryjne otwieranie wszystkich szlabanów na wypadek sytuacji specjalnych za pomocą przycisku ROP umieszczonego w recepcji .

Szlabany będą o szerokości max 4 m. Jeden na wjazd drugi na wyjazd. Ze względu na małą szerokość wjazdu możliwą do zagospodarowania, nie ma możliwości wykonania tzw. wysepki.

Dla wejścia pieszego w rejonie uzgodnionym z Zamawiającym wykonany zostanie system KD który będzie zamontowany z tzw. timerem. Drzwi (bramka) będzie otwarta cały dzień - utrzymywana za pomocą magnetycznych trzymaczy drzwiowych. Po określonej godzinie trzymacze zwalniają zaczepy i wejście będzie możliwe tylko za pomocą karty systemu KD..

W rejonie wjazdu/wyjazdu z parkingów położona zostanie kostka na wcześniej przygotowanym podłożu (kruszywo)-umieszona będzie pętla indukcyjna sterująca wyjazdem pojazdu (swobodny wyjazd) .

Bramy do wymiany z zapewnieniem zachowania symbolu wraz z montażem siłownika.

System wraz z licencjami uruchomiony będzie na dedykowanych serwerach KD oraz CCTV/VMS.

Zakres prac podstawowych wraz z urządzeniami	***2ilość***
Szlabany 4 m (200 cykli /h)	*6*
System otwieranie szlabanów za pomocą aplikacji mobilnej	*4*
Bramka wejściowa ,samozamykacz, czytnik KD, trzymacz drzwiowy	*1*
Przygotowanie podłoża w rejonie wyjazdu z parkingów ok 8 na 4m (32m2)	*2*
Pętla indukcyjna	*4*
Okablowanie	*1*
Domofony	*3 kpl*
Brama wjazdowa wraz z siłownikiem	*3*
Siłownik	*4*
Prace montażowe i uruchomienie	*1*
Stanowisko operatora +monitor 24"	*1*
Urządzenia , licencje , wdrożenia C&C, serwer VDG Sense	*1 kpl*

System zarządzania dostępem do obiektu.

Wszystkie systemy bezpieczeństwa zainstalowane w obrębie Wojewódzkiego Szpitala Specjalistycznego nr 4 w Bytomiu muszą być w pełni monitorowane i zarządzane z poziomu centralnej platformy Systemu Zarządzania Bezpieczeństwem (SMS). Ogólne założenia opracowane zostały na podstawie odpowiednich norm i przepisów:

- PN-EN 50133 – w zakresie Kontroli Dostępu;
- PN-EN 50132 – w zakresie Systemów Telewizji Dozorowej.

Platforma zarządzania SMS umożliwia wzajemne współdziałanie poniższych podsystemów za pomocą

interfejsów programowych:

- Kontroli Dostępu,
- Monitoringu Wizyjnego CCTV IP,
- Zarządzania Parkingiem.

Dodatkowo system SMS musi umożliwiać rozbudowę i integrację systemów m.in.:

- Sygnalizacji Włamania i Napadu,
- Interkomowego SOS/INFO,
- Depozytorami kluczami,
- Sygnalizacji Pożarowej,
- Automatyki.

Każda z funkcjonalności musi być dostępna zarówno na etapie projektu i wdrażania, jak i ewentualnej rozbudowy działającego systemu. Dodatkowo każdą z funkcjonalności oraz każdy z modułów będzie można płynnie rozbudowywać w przyszłości.

System Zarządzania Bezpieczeństwem (SMS) powinien być oparty na strukturze sieci IP z centralnym serwerem SMS oraz rozproszoną strukturą elementów sterujących, wykorzystującą standardowe łącza okablowania strukturalnego, zarówno miedzianego jak i światłowodowego. Każdy sterownik musi posiadać możliwość nadzorowania prawidłowego działania za pomocą sieci LAN i musi działać w trybie Plug-Play.

Aplikacja SMS musi być oparta na technologii Web i umożliwiać dostęp użytkownikom do interfejsu systemu za pomocą przeglądarek internetowych Internet Explorer, Chrome lub Firefox z dowolnej stacji operatorskiej podłączonej do sieci bezpieczeństwa (lokalnie lub zdalnie, np. za pomocą wirtualnej sieci lokalnej VPN). Ze względów bezpieczeństwa, dostęp nie może wymagać instalacji jakiegokolwiek oprogramowania lokalnie na stacji operatorskiej. Musi działać zarówno w środowisku Unix, jak i Windows bez żadnych ograniczeń funkcjonalnych.

WYMAGANIA PODSTAWOWE

1. Neutralność maszyny serwerowej.

   System KD musi być neutralny względem producenta maszyn serwerowych, centrali głównej tzn.:
   a) system musi posiadać wsparcie dla serwerów fizycznych zgodnych z architekturą 64 bitową,
   b) spełniać minimalne wymagania parametrów technicznych podanych w karcie katalogowej aplikacji,
   c) producent systemu KD musi mieć możliwość dostarczenia tylko oprogramowanie i licencji.

2. Active Directory (AD).
   System KD musi zapewniać możliwość synchronizacji użytkowników oraz uprawnień z systemem nadrzędnym Active Directory (AD):
   a) Na podstawie informacji z AD dane użytkowników w SKD muszą być aktualizowane automatycznie w ważność ich dostępu odpowiednio modyfikowana;
   b) Aktywacja lub dezaktywacja konta w AD musi powodować odpowiednio przyznanie lub zablokowanie ważności kart w SKD;
   c) Zmiana danych (imienia lub nazwiska) w AD musi zmienić dane powiązanego użytkownika w SKD pozostawiając jednocześnie jego uprawnienia;
   d) Usunięcie użytkownika AD musi spowodować wyłączenie wszystkich kart danej osoby w SKD;
   e) Dodanie nowego użytkownika w AD musi spowodować utworzenie nowej osoby

w SKD bez przypisanych kart;

f) Synchronizacja SKD z AD musi umożliwiać synchronizację uprawnień dostępu do czytników/grupy czytników.

3. System SKD musi być zgodny z EN 60839 GRADE3
   - Logowanie prób wyświetlania, drukowania logów systemu KD przez operatora.

     Zgodnie z wymaganiem normy EN60839-11 Grade 3 i 4 system musi posiadać mechanizm audytu/logowania informacji, który operator szukał, wyświetlał dane historyczne systemu KD. Dane, które mają się logować to minimum ID operatora oraz data i godzina wyszukiwania zdarzeń.

4. Platforma KD musi być skalowalna i umożliwiać realizacji rozbudowanych instalacji. Ze względu na to platforma KD:
   - musi umożliwiać dodanie co najmniej 150 000 użytkowników do systemu przypisanych do co najmniej 1 024 grup użytkowników;
   - musi pozwalać na zapisanie w systemie co najmniej 7 000 000 zdarzeń;
   - musi umożliwiać dodanie co najmniej 3 200 map synoptycznych oraz 32 000 obiektów;
   - nie może ograniczać liczby stanowisk operatorskich.

KONFIGUARACJA SPRZĘTOWA

Sterownik sieciowy

- Szyfrowana komunikacja AES256 między sterownikiem a serwerem;
- System operacyjny LINUX;
- Montaż na szynę DIN 35 mm;
- Pobór mocy (średnio 2.5W);
- Zasilanie 12 – 24 V DC;
- Możliwość podłączenie do 4 kontrolerów w trybie End To End Security (szyfrowanie od karty do serwera);
- Obsługa wielu interfejsów i topologii: Wiegand, RS232, RS485, Clock/Data, TCP/IP, gwiazda i magistrala.

Kontroler drzwiowy

- Praca w architekturze gwiazdy, magistrali lub stacku;
- Obsługa min. 2 czytników kontroli dostępu;
- Wbudowany moduł min. 8 wyjść;
- Wbudowany min. 6 wejść monitorowanych i 2 wejść cyfrowych,
- Obsługa min. 2 mierników temperatury / wilgotności
- Wysoka gęstość instalacji (montaż DIN)

Środowisko serwerowe

Maszyna na jakiej ma być docelowo zainstalowane oprogramowanie powinna posiadać poniższą lub wyższą specyfikację techiczno-sprzętową:

- procesor - x Intel Xeon E3-1220 v5 @ 3.0GHz
- obudowa - 3,5" z maks. 2 dyskami twardymi
- moduły RDIMM 2666MT/s
- 4GB pamięci UDIMM, 2400MT/s,
- 1TB 7.2k RPM SATA 6Gbps 3.5"
- DVD ROM napęd SATA wewnętrzny
- zasilacz 250W
- karta sieciowa

System ma umożliwić podłączenie następujących urządzeń do sterownika sieciowego lub kontrolera drzwiowego:

1. czytnik komunikujący się poprzez protokół Wiegand, RS482, RS232,
   Wyżej wypisane elementy muszą posiadać możliwość współpracy z kartami dostępowymi kompatybilnymi z Mifare 1K, Mifare 4K, Mifare DESFire 0.6, Mifare DESFire EV1 8K oraz zgodnymi z ISO14443A. System ma zapewniać kompatybilność z kartami zamawiającego.
2. system ma mieć możliwość integracji z systemem depozytorów kluczy istniejących na obiekcie.

FUNKCJE SYSTEMU

1. Funkcję globalnego Anti-Pass Back z podziałem na strefy (wsparcie dla Anti-Pass Back globalnie, punktowo, czasowo, rewersyjnie).
2. Funkcję śluzowości obsługującą do 16 wejść.
3. Funkcję kwarantanny, która zabrania użytkownikom wejście do określonych stref, jeżeli wcześniej znajdowali się w innej, ściśle zdefiniowanej strefie.
4. Funkcję nadawania praw użytkownikom, w momencie gdy znajdowali się w innej strefie, np. karta jest ważna na terenie magazynu, tylko w momencie gdy wcześniej została użyta w portierni.
5. Funkcję wejścia pod przymusem polegającą na zapisaniu dla danego użytkownika dwóch haseł pin. W momencie gdy dany użytkownik wchodzi pod przymusem do strefy, przykłada kartę i wpisuje hasło dedykowane dla wejścia pod przymusem. Uzyskuje on dostęp do danej strefy, jednocześnie operator zostaje powiadomiony o fakcie wejścia pod przymusem.
6. Funkcję rozbudowanych alarmów kontroli dostępu, w których alarm jest wzbudzony w momencie gdy karta zostaje uznana jako skradziona, lub użytkownik przyłoży do kartę do czytnika do którego nie ma uprawnień.
7. System KD musi umożliwiać automatyczne wylogowywane operatora (AWO) w przypadku braku aktywności w aplikacji do zarządzania KD. Minimalne wymagania:
   - Możliwość aktywacji funkcji AWO dla wszystkich lub wybranych użytkowników systemu;
   - Możliwość przypisania indywidualnego czasu „braku aktywności" dla każdego użytkownika/ operatora podawanego w minutach;
   - Minimalny czas braku aktywności to 1 minuta;
   - Maksymalny czas braku aktywności operatora musi wynosić 1 rok lub więcej.

8. Funkcja redundancji

   System KD ma umożliwiać rozbudowę o funkcję serwera redundantnego, który może działać w trybie cold standby lub hot standby.
   W przypadku awarii serwera podstawowego i automatycznej aktywacji serwera redundantnego wymagane jest poinformowania operatora o fakcie, że system działa na serwerze redundantnym.

9. Moduł Gościa

   System KD musi posiadać moduł Gościa (Vistor).
   Minimalne wymagania funkcjonalne:
   - Status gościa w systemie KD to minimum: Zgłoszony, przybył, obecny;
   - Możliwość automatycznego poinformowania za pomocą maila „opiekuna gościa" o przybyciu gościa na obiekt w momencie:
     a) zmiany status gościa z poziomu aplikacji recepcji,
     b) użycia karty gościa na czytniku KD.

10. Integracja z VMS:

System musi być zintegrowany z systemem VMS (Video Management System) za pośrednictwem dedykowanego licencjonowania.

11. Tablice rejestracyjne:

    Projektowany system i dostarczone wraz z nim oprogramowanie musi umożliwić dodanie tablic rejestracyjnych pojazdów oraz musi posiadać dostęp do systemu VMS, który umożliwi pozyskanie danych a także numerów tablic rejestracyjnych pojazdów pozyskanych z modułów sprzętowych podłączonych bezpośrednio do system kontroli dostępu.

12. System awizacji:

    Oprogramowanie do zarządzania systemem powinno mieć wydzielony moduł specjalnie do realizacji wizytacji gości na obiekcie. Moduł ten powinien posiadać możliwość:
    - dodawania osoby,
    - dodawania karty,
    - dodawania uprawnień pojedynczo i grupowo,
    - raportu wejść i wyjść karty po czytniku i po karcie,
    - awizacja gości.

Skalowalność systemu:
Platforma KD musi być skalowalna i umożliwiać realizacji rozbudowanych instalacji. Ze względu na to platforma KD:
- musi umożliwiać dodanie co najmniej 150 000 użytkowników do systemu przypisanych do co najmniej 1 024 grup użytkowników;
- musi pozwalać na zapisanie w systemie co najmniej 7 000 000 zdarzeń;
- musi umożliwiać dodanie co najmniej 3 200 map synoptycznych oraz 32 000 obiektów;
- nie może ograniczać liczby stanowisk operatorskich.

RODO OCHRONA DANYCH OSOBOWYCH
Zgodnie z RODO dane osobowe muszą być chronione przed wszelkimi przypadkami nadużycia w najlepszym możliwy sposób. Dane osobowe mogą być zapisane w bazie danych SKD, z tego powodu baza danych i kopia zapasowa bazy danych musi być zabezpieczona przed wyciekiem danych.
SKD musi zapewniać odpowiednie mechanizmy zabezpieczające:
- dane osobowe w kopii zapasowej SKD nie mogą być odczytywane przez osoby nieupoważnione;
- kopia bazy danych musi być zaszyfrowana;
- kopia bazy danych musi być zabezpieczona przed możliwością odczytu, importu i przywrócenia na innym serwerze SKD bez kluczy szyfrujących z serwer podstawowego;
- SKD musi posiadać dziennik logów, z informacją, kto żąda kluczy szyfrujących, aby przywrócić bazę danych;
- kopia zapasowa SKD może być używana przez serwery redundantne automatycznie bez ograniczeń;
- backup techniczny – Do celów serwisowych musi istnieć możliwość utworzenia kopii zapasowej bez informacji poufnych.

W kontekście RODO procesy systemowe muszą być identyfikowalne z osobą.
Z tego powodu w systemie KD musi istnieć możliwość nadania praw „super użytkownika” do każdej osoby indywidualnie, która posiadać uprawnienia administratora, mając prawo do tworzenia i zarządzania użytkownikami systemu. Super użytkownik musi być identyfikowany z imienia i nazwiska a jego operacje logowane a dzienniku zdarzeń.

System zarządzania video VMS telewizji przemysłowej CCTV IP

System ma być oparty na technologii IP. Obraz z kamer ma być nagrywany przez serwery wideo. System ma być zgodny minimum z poziomem Grade 3 wg normy PN-EN 62676-1.
System ma się składać z:

- 4 kamery 5MPXo ogniskowej 2,7mm-13mm zewnętrzne wyposażonych w obudowę z grzałką, promiennikiem;
- 3 kamery (LPR) 2MPX o ogniskowej 8mm-32mm;
- Funkcja analityki obrazu rozpoznawania tablic rejestracyjnych dla 4 punktów kamerowych;
- Serwera rejestrującego video;
- 1 stanowisko operatorskie (wspólne dla platformy SMS/CCTV).

Architektura systemu: musi być zbudowana w modelu klient- serwer, z zastosowaniem architektury rozproszonej serwerów z zasilaczami redundantnymi oraz macierzami DAS pracującymi w trybie RAID (opcje konfiguracji: 0,1, 5, 6, 10, 50, 60).
Aplikacja serwerowa platformy musi wspierać architekturę 64-bitową, ma zapewnić obsługę min. 320 kamer w rozdzielczości FullHD w trybie zapisu ruchu na jednej jednostce serwerowej, z wydajnością min 700 Mbit/s.

Serwer ma zarządzać następującymi komponentami platformy:

- grupami użytkowników oraz użytkownikami;
- alarmami z poszczególnych serwerów;
- makrami;
- uprawieniami poszczególnych grup użytkowników;
- układami widoków, multi-widoków wraz z przypisanymi do nich urządzeniami z poszczególnych serwerów slave;
- sekwencjami kamer;
- harmonogramami nagrywania i archiwizacji;
- wtyczkami (Plug-in) odpowiadającymi za komunikację pomiędzy platformą, a systemami firm trzecich, takimi jak zewnętrzna analityka wideo, system ochrony obwodowej itd.;
- modułem API HTTP łączącym platformę z dowolną aplikacją lub interfejsem, który został stworzony z jego wykorzystaniem w celu integracji z platformą;
- przydzielonymi kamerami i koderami oraz archiwizowanie wideo / audio;
- urządzeniami zewnętrznymi np. audio, wejście, wyjścia, porty szeregowe; sterowanie PTZ.

Platforma musi zapewnić obsługę min 33 producentów kamer i koderów na bazie autorskich dedykowanych protokołów tych producentów, aby zapewnić jak największą elastyczność oraz możliwość doboru jak najlepszego urządzenia spełniającego wymagania ekspozycji, transmisji itp. w danym punkcie kamerowym.
System musi zapewniać możliwość implementacji w systemie wirtualizacyjnym min. VMWare, Microsoft Hyper-V.

Środowisko serwerowe
Maszyna na jakiej ma być docelowo zainstalowane oprogramowanie powinna posiadać min.:

- procesor Intel Xeon E2200
- 16GB pamięci RAM
- Dysk SSD 128 GB
- 2 x GB Ethernet - karta sieciowa
- system operacyjny Microsoft Windows 10 Pro 64-bit
- obsługa RAID 5
- 4 zatoki na dyski 3,5” (hot swap)
- Zasilacz 400W
- Montaż dysków o maksymalnej pojemności 18TB każdy.

Wymagany czas archiwizacji obrazu z kamer to minimum 14dni.

System ma umożliwiać przywracania danych z kart SD w kamerach zgodnie z opisem standardu Onvif G.
W przypadku utraty połączenie między serwerem VMS a kamerą, kamera powinna wykryć utratę strumienia połączenia RTPS i na tej podstawie rozpocząć nagrywanie na dołączonej karcie SD. Po powrocie połączenia z serwerem, na liście zdarzeń operatora systemu VMS ma pojawić się informacja, o dostępności materiałów do pobrania z kart SD w kamerach i uzupełnienie brakującego materiału video z okresu braku komunikacji między serwerem, a kamerą.
System musi zapewniać dedykowane menu z listą zdarzeń przedstawiającą:

- dokładny okres, w którym występował brak komunikacji między kamerą a serwerem aktualny status kamery;
- akcje do wykonania przez operatora: synchronizuj pojedynczą kamerę, synchronizuj wszystkie kamery i wszystkie okresy, usuń z listy wszystkie okresy, wstrzymaj pobieranie z pojedynczej kamery, wstrzymaj pobieranie z wszystkich kamer;
- pasek postępu synchronizacji danych.

System musi umożliwiać synchronizację i uzupełnianie danych nawet gdy strumień nagrywany na serwerze i na karcie SD znacznie się różnią np. rozdzielczością, ilością klatek.

System zapewni możliwość wyszukiwania zdarzeń dostępności danych do pobrania oraz problemów z kartą SD (błąd zapisu z wykorzystaniem narzędzi wyszukiwania zdarzeń w systemie w jego bazie SQL, a także możliwość stworzenia reakcji przez makro na zdarzenia minimum wysłanie e-maila, przekazanie informacji do systemu PSIM, przełączenie widoku operatora i poinformowanie go o wydarzeniu).

Obsługa operatorska – system musi zapewniać nieograniczoną licencyjnie ilość jednoczesnych połączeń klienckich z komputerów zdalnych wyposażonych w aplikacje kliencką systemu, urządzeń mobilnych obsługiwanych przez system Android lub iOS oraz z przeglądarki internetowej.

Ze względu na wrażliwe dane jakimi będą nagrania, system nie powinien umożliwiać operatorom dowolnego eksportu i kopiowania nagrań. Eksport i kopiowanie nagrań powinno być możliwe tylko w przypadkach uzasadnionych i powinno być autoryzowane przez dwóch użytkowników systemu, a mianowicie operatora i administratora (kierownika) przez tzw. Funkcjonalność dualnego logowania.

System musi zapewniać możliwość importu użytkowników do systemu z usług katalogowych systemu min. Active Directory i LDAP oraz wykorzystanie mechanizmów jednorazowego logowania do systemu tzw. SSO.

Rozpoznawanie tablic rejestracyjnych: algorytm skanuje tablice rejestracyjne wprost z bieżącego strumienia wideo i klasyfikuje znalezioną tablicę przypisując ją do kraju, w którym pojazd jest zarejestrowany. Znalezione tablice mogą być porównywane z tzw. czarną i białą listą dostępową w wyniku czego generowane są zdarzenia z automatycznym przypisaniem reguły odpowiednich makr, np. moduł I/O aktywuje otwarcie szlabanu po wykryciu przez system obecności pojazdu uprawnionego do wjazdu na teren chronionego obiektu. Aktywacja profilu wykrywającego pojazdy opuszczające parking w zdefiniowanym okresie czasu pozwala na wspomaganie procesu zarządzania wolnymi miejscami.
Cechy analizy tablic rejestracyjnych:

- Programowa korekta geometryczna dla scenariuszy nieoptymalnego kąta montażu kamer;
- Eksport / import danych do szeregu typu plików w tym min. CSV, przez zapytania SQL;
- Autoryzacja dostępu na bazie harmonogramów w korelacji z białymi, czarnymi listami dostępu;
- Korelacje rozpoznania tablic (specyficznej tablicy lub grupy tablic) z dowolną akcją;
- Obsługiwanie przez system makr min.: otwarcie bram, szlabanów, alarmowanie operatora przez przełączenie widoku, wysłanie maila ze zdjęciem itd., realizacja odpowiedniej sekwencji procedury polityki bezpieczeństwa;
- Zapis danych w bazie danych SQL oraz materiału video i zdjęć MJPEG rozpoznanych tablic pojazdów na podstawie kryterium czasowego, lokalizacji;
- Przekazywanie danych o rozpoznanych tablicach dla systemów integrujących w tym min. do systemów zarządzania bezpieczeństwem systemu SMS (wielostopniowa weryfikacja dostępu do obiektu w scenariuszu lokalnym i scentralizowanym), systemów parkingowych itd.;
- Łatwość filtrowania zdarzeń dla konkretnej tablicy, grupy tablic.

Parametry techniczne kamer:

Kamery do rozpoznawania tablic rejestracyjnych	
Przetwornik obrazu	1 / 1,8 " CMOS dla ultra słabego oświetlenia
Obiektyw	Zmotoryzowany 8 do 32mm, F/1.6
Fokus	Autofokus, Pół-automatyczny, ręczny
Pole widzenia	42.5° do 13.4° w poziomie
Min. natężenie oświetlenia	Kolor: 0.002 lux, Czarny/Biały: 0.0004 lux (F/1.2 AGC ON)
Tryb dzień/noc	Filtr podczerwieni z automatycznym przełącznikiem
Zasięg promiennika IR	do 100 m
Długość fali promiennika IR	850 nm
WDR	140 dB
Szybkość migawki	Od 1 s do 1/100,000 s
Wolna migawka	Obsługiwana
Wyzwalacz alarmu	Wykrywanie ruchu, alarm sabotażu, odłączenie sieci,konflikt adresu IP, nielegalne logowanie, dysk pełny,błąd dysku, Tablice rejestracyjne na białej i czarnej liście
Wejście alarmowe	2x wejścia
Wyjście alarmowe	2x wyjścia (do 24Vdc 1A lub 110Vac 500mA)
Pamięć sieciowa	NAS (NFS, SMB/CIFS), ANR
Zapis video w urządzeniu	Wbudowany slot mikro SD/SDHC/SDXC , do 256 GB

Zasilanie	12Vdc 20% (kostka), PoE (802.3at kasa 4)
Pobór mocy	1.2A maks., Maks. 14 W
Klasa szczelności	IP67
Ochrona przed uderzeniami	IK10
Temperatura robocza	od -30°C do +60°C
Wilgotność względna	+ 5% do 100%

Kamery monitorujące parking	
Czujnik obrazu	Progresywny CMOS 1/2,7"
Pixele	2592x1944(5MP)
Tryby pracy	Wykrywanie ruchu, alarm sabotażowy, wejścia/wyjścia alarmowe, zdarzenia Smart Analytics
Minimalne oświetlenie	Kolor: 0,003 luksa, czarno-biały: 0 luksów, 0 luksów przy włączonym oświetleniu IR, F1,4
Obiektyw	Zmotoryzowany 2,7 do 13,5 mm, Auto-iris
Fokus	Autofokus
Pole widzenia	od 32° do 103° w poziomie, od 24° do 73° w pionie
Tryb dzień/noc	Filtr podczerwieni z automatycznym przełącznikiem
Szybkość migawki	od 1/3 s do 1/100 000 s
Wolna migawka	Obsługiwana
Kontrola szybkości transmisji/kompresji	Stała przepływność (CBR), zmienna przepływność (VBR), Smart Bitrate (H.265+, H.264+)**
Liczba strumieni wyjściowych wideo	Do 6 (RTSP)
Szeroki zakres dynamiczny	120dB
Balans bieli	Automatyczny (3 poziomy), stały, ręczny
Ustawienia obrazu	Nasycenie, jasność, kontrast, ostrość, kompensacja podświetlenia, kompensacja podświetlenia, WDR, kontrola ekspozycji, wzmocnienie, kompensacja podświetlenia
Ulepszanie obrazu	3DNR, odmgławianie
Kompresja wideo	H.265 (Main Profile) / H.264 (High Profile/Main Profile/High Profile) / MJPEG
Częstotliwość wyświetlania klatek	25/30 kl/s
Maksymalna transmisja strumieniowa - 25kl/s	2592x1944, 640x480
Maksymalna transmisja strumieniowa - 25kl/s*	2592x1944, 640x480, 1920x1080, 1280x720
Maksymalna transmisja strumieniowa - 30kl/s*	2688x1520, 640x360, 1280x720
SNR	52dB
Szybkość transmisji wideo	32Kbpf do 16Mbps
Maksymalna rozdzielczość	2592x1944 25 kl/s
Wspierana rozdzielczość	2592x1944, 2699x1520, 1920x1080, 1280x720, 640x480, 640x360
Przełącznik dzień/noc	Automatyczne/ Zaplanowane/ Wyzwalane przez wejście alarmu

Wykrycia zdarzeń	Wejście zewnętrzne, wyjście zewnętrzne, sabotaż, wykrywanie dźwięku, wyzwalanie ręczne, powiadomienie o nagraniu, rozłączenie sieci, konflikt adresów IP, nielegalne logowanie
Akcja zdarzenia	Wyjście alarmowe, nagrywanie klipu wideo na kartę NAS/SD, Wysyłanie wiadomości alarmowej i obrazu przez e-mail/FTP, wysyłanie powiadomienia HTTP
Analiza	Przekroczenie linii, detekcja wtargnięcia, detekcja wyjścia z obszaru, opuszczony obiekt, usuwanie obiektów
Protokoły sieciowe	IPv4/IPv6, HTTP, HTTPS (TLS1.2), 802.1x, Qos, FTP, SMTP(SSL), UPnP,SNMP(v1/v2/v3/Traps), DNS, DDNS, NTP, RTSP, RTCP, RTP/UDP, TCP/IP, IGMP(v2/v3),DHCP, PPPoE, SSL/TLS, ONVIF Profile S/G/T, Protokół Siqura, ISAPI
Bezpieczeństwo	Uwierzytelnianie użytkowników, zarządzanie uprawnieniami, uwierzytelnianie szyfrowane (RTSP, HTTP),szyfrowanie HTTPS (TLS1.1/1.2); Kontrola dostępu do sieci w oparciu o port IEEE 802.1x, filtrowanie IP
Interfejs komunikacyjny	10/100 Mb (RJ45)
Interfejs audio	1x wejście audio 3,5 mm (wejście liniowe), amplituda 3,3 Vpp, impedancja 4,7 K; 1x wyjście audio 3,5 mm, amplituda 3,3 Vpp, impedancja 100
Kompresja	G.711, G.726, AAC, PCM
IR	Diody IR 850nm, widoczna długość IR 60m
Stopień ochrony	IP67, IK10
Temperatura robocza	od -30°C do +60°C
Wilgotność względna	95% lub mniej, bez kondensacji

System parkingowy

Zakłada się zainstalowanie na wjeździe/ wyjeździe z parkingu systemu kontroli wjazdu/ wyjazdu.

System musi realizować również autoryzację wjeżdżającego pojazdu poprzez rozpoznanie tablic rejestracyjnych za pomocą kamery monitoringu . System musi pozwalać na realizację autoryzacji wjeżdżającego auta w oparciu o następujące kombinacje autoryzacji:

- Karta systemu kontroli dostępu,
- Rozpoznanie numeru tablicy rejestracyjnej przez kamerę systemu CCTV,
- Kartę kontroli dostępu lub rozpoznawanie tablicy przez kamerę systemu CCTV,
- Kartę kontroli dostępu i rozpoznawanie tablicy przez kamerę systemu CCTV,
- Za pomocą aplikacji mobilnej.

System kontroli wjazdu dla pracowników musi wymieniać informacje w czasie rzeczywistym z Systemem Zarządzania Bezpieczeństwem, sygnalizującym na bieżąco stan szlabanu i rejestrujący w systemie poszczególne wjazdy ma teren Szpitala.

Aplikacja do administrowania uprawnieniami użytkowników, awizacji wjazdów, zarządzeniem listami pojazdów z wykorzystaniem systemu Kontroli Dostępu oraz CCTV. Interfejs graficzny pozwala administratorowi na szybkie założenie użytkownika, przypisanie kart zbliżeniowych oraz tablic rejestracyjnych z jednoczesnym zdefiniowaniem zasobów obiektu, do których dany użytkownik powinien posiadać dostęp.