**Znak sprawy: OZP.261.23.2022.ŁF Załącznik nr 8 do SWZ**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

1. Przedmiotem zamówienia jest dostawa, montaż, uruchomienie oraz świadczenie serwisu urządzeń (wraz z materiałami eksploatacyjnymi) w okresie gwarancji (minimum 2 lata) do kontroli dostępu (8 przejść jednostronnych, 1 – dwustronnie z barierą podczerwieni,
1 – windowe) i rejestracji czasu pracy (z terminalem rejestracji czasu pracy) oraz dostawa wraz z integracją, wizualizacją, wdrożeniem i uruchomieniem niezbędnego oprogramowania do zarządzania kontrolą dostępu (w tym również szkolenie i serwis) w budynku biurowy Regionalnego Ośrodka Polityki Społecznej w Rzeszowie.
2. Wykonawca w ramach realizacji zamówienia o którym mowa w pkt. 1 zobowiązuje się do montażu automatycznych bramek uchylnych, które zastosowanie mają do przejść dla osób niepełnosprawnych, przejść ewakuacyjnych lub technicznych. Przeznaczone są do pracy w warunkach, które nie są narażone na działanie czynników atmosferycznych. Wyposażone są w mechanizm dwukierunkowy oraz piktogramy informacyjne. Wygrodzenie pozostałej przestrzeni przy bramkach uchylnych możliwe jest przy pomocy słupków i barierek wygrodzeniowych. Obudowa i ramiona bramki oraz słupki i barierki wygrodzeniowe standardowo wykonane są ze stali nierdzewnej natomiast skrzydła uchylne bez ramek ze stali nierdzewnej wykonane ze szkła hartowanego (przeźroczyste/mleczne).
3. Przedmiot zamówienia zostanie dostarczony fabrycznie nowy, zainstalowany, uruchomiony oraz świadczony będzie serwis w następującej lokalizacji:

Regionalny Ośrodek Polityki Społecznej w Rzeszowie przy ul. Hetmańskiej 9, 35-045 Rzeszów zlokalizowany na działce nr 1375/4 w obrębie 207 Rzeszów.

1. Zamawiający umożliwia i zaleca przeprowadzenie tzw. wizji lokalnej w ww. lokalizacji, po uzgodnieniu terminu w celu prawidłowego przygotowania oferty oraz zweryfikowania możliwości zintegrowania obecnie funkcjonujących w obiekcie systemów (t.j. SAP-SSP - system bezpieczeństwa sygnalizacji pożarowej w tym oddymiania, CCTV - system bezpieczeństwa nadzoru wizyjnego – telewizyjnego, SSWiN - system bezpieczeństwa włamania i napadu) z planowanymi do wdrożenia systemami.

Przeprowadzenie wizji lokalnej możliwe będzie w godz. 8.30-14.30.

1. Wykonawca w ramach realizacji zamówienia, o którym mowa w pkt. 1 zobowiązuje się do dostawy, montażu, uruchomienia urządzeń do kontroli dostępu i rejestracji czasu pracy oraz dostawy niezbędnego oprogramowania do zarządzania kontrolą dostępu i instalacji okablowania, listew kablowych, konfiguracji urządzeń, a także naprawy elementów ścian, podłóg, sufitów po prawidłowej instalacji urządzeń wchodzących w skład zamówienia.
2. Wykonawca zobowiązuje się posprzątać pomieszczenia po zakończeniu prac związanych instalacją urządzeń wchodzących w skład zamówienia oraz zutylizować wszelkie opakowania na własny koszt.
3. Zamawiający informuje, że system będzie wykorzystywany przez min. 100 pracowników, z możliwością obsługi min 250 kart. W zakresie przedmiotu zamówienia Wykonawca musi dostarczyć 250 kart.
4. **ELEMENTY SYSTEMU**
	1. KD - system kontroli dostępu wraz rejestracją czasu pracy;
	2. CCTV - system bezpieczeństwa nadzoru wizyjnego – telewizyjnego;
	3. OIB - system oprogramowania integracyjnego bezpieczeństwa oraz inne aplikacje, zamontowany i wdrożony dla niezbędnych danych w funkcjonalności bezpieczeństwa budynku i ludzi, w tym sygnały/zmienne dla alarmów, K-krytycznych, O-ostrzegawczych i D-diagnostycznych w zakresie niezbędnych funkcjonalności tj. np. SAP - alarm I i II stopnia, awaria systemu zasilania, uszkodzenie czujki;
	4. SAP-SSP- system bezpieczeństwa sygnalizacji pożarowej w tym oddymiania;
	5. SSWiN - system bezpieczeństwa włamania i napadu;
5. **ZASTOSOWANE MATERIAŁY**
	1. Ogólne wymagania - materiały użyte do wykonania instalacji muszą spełniać wymagania niniejszej specyfikacji. Możliwe jest zastosowanie produktów równorzędnej jakości po akceptacji Zamawiającego. Jakiekolwiek zmiany w realizacji przedmiotu zamówienia tj. przeróbki instalacyjne muszą być wykonane w uzgodnieniu z Zamawiającym i na koszt Wykonawcy. Wszystkie materiały powinny odpowiadać wymaganiom zawartym w dokumentach odniesienia (normach, aprobatach technicznych):
* PN-EN 62208:2011 Puste obudowy rozdzielnic i sterownic niskonapięciowych -- Wymagania ogólne;
* PN-EN 61914:2009 Uchwyty przewodów do instalacji elektrycznych;
* PN-EN 61439-1:2010 Rozdzielnice i sterownice niskonapięciowe -- Część 1: Zestawy badane w pełnym i niepełnym zakresie badań typu;
* PN-EN IEC 60799:2021-07 Sprzęt elektroinstalacyjny -- Przewody przyłączeniowe i przewody pośredniczące;
* PN-EN 62208:2006 Puste obudowy rozdzielnic i sterownic niskonapięciowych -- Wymagania ogólne;
* PN-E-93208:1997 Sprzęt elektroinstalacyjny -- Puszki instalacyjne;
	1. Deklaracja zgodności

Wyroby i materiały elektryczne winny spełniać warunki określone Ustawą dnia 16 kwietnia 2004 r. o wyrobach budowlanych ([Dz. U. z 2021 poz. 1213)](https://sip.lex.pl/#/act/17091527/2961714) potwierdzone wymaganymi dokumentami zgodnie z Rozporządzeniem Ministra Infrastruktury i budownictwa z dnia 17 listopada 2016 r. w sprawie sposobu deklarowania właściwości użytkowych wyrobów budowlanych oraz sposobu znakowania ich znakiem budowlanym Dz.U. z 2021 poz. 2260 i powinny posiadać aktualny certyfikat na znak bezpieczeństwa. Wykonawca zapewni, aby tymczasowo składowane materiały, do czasu, gdy będą one potrzebne do prac, były zabezpieczone przed zniszczeniem, zanieczyszczeniem, zachowały swoją jakość i właściwość.

* 1. Rozdzielnice obiektowe

Zasilane elementy będą wykonane z istniejących rozdzielnic. Rozdzielnice niskiego napięcia będą opracowane i wykonane zgodnie z Polskimi Normami oraz opisem technicznym.

* 1. Instalacja tras kablowych

Trasy kablowe należy rozumieć jako kładzenie przewodów w rurkach instalacyjnych we wcześniej wykutych trasach kablowych zgodnie z opisem technicznym. Wszelkie zakręty należy wykonywać po łuku aby nie „złamać” przewodu. Wszystkie przewody należy sprawdzić i wykonać protokół pomiarowy.

* 1. Wprowadzanie przepustów kablowych

Końce rur należy zabezpieczyć dedykowanymi do tego celu uszczelnieniami systemowymi.

1. **SPRZĘT**

Wykonawca jest zobowiązany do używania jedynie takiego sprzętu, który nie spowoduje niekorzystnego wpływu na jakość wykonywanych prac, zarówno w miejscu tych prac, jak też przy wykonywaniu czynności pomocniczych oraz w czasie transportu, załadunku i wyładunku materiałów, sprzętu itp. Sprzęt używany przez Wykonawcę powinien uzyskać akceptację Zamawiającego. Liczba i wydajność sprzętu powinna gwarantować wykonanie prac zgodnie z zasadami oraz w przewidzianym terminie.

1. **TRANSPORT MATERIAŁÓW**

Wykonawca jest zobowiązany do stosowania jedynie takich środków transportu, które nie wpłyną niekorzystnie na jakość wykonywanych prac. Urządzenia transportowe powinny być odpowiednio przystosowane do przewozu elementów, konstrukcji itp. niezbędnych do wykonania prac. Przewożone środkami transportu elementy powinny być zabezpieczone przed ich uszkodzeniem, przemieszczaniem i w opakowaniach zgodnych wymaganiami producenta.

1. **WYKONYWANIE PRAC**
	1. Zaginanie kabli i przewodów

Przy układaniu kabli można zginać kabel tylko w przypadkach koniecznych, przy czym promień gięcia powinien być możliwie duży, nie mniejszy niż podany przez producenta. Jeżeli jest brak danych to promień gięcia nie powinien być mniejszy niż określony w N SEPE-004 p-kt. 2.5.3.

* 1. Montaż skrzynek niskoprądowych

Montaż skrzynek należy wykonać zgodnie z wytycznymi oferowanego producenta.

* 1. Przejścia przez ściany

Wszystkie przejścia obwodów instalacji elektrycznych i niskoprądowej przez ściany, itp. muszą być chronione przed uszkodzeniami. Przejścia wymienione powyżej należy wykonać w przepustach rurowych. Przejścia między pomieszczeniami o różnych atmosferach powinny być wykonane w sposób szczelny, zapewniający nie przedostawanie się wyziewów. Obwody instalacji elektrycznych przechodzące przez podłogi muszą być chronione do wysokości bezpiecznej przed przypadkowymi uszkodzeniami. Jako osłony przed uszkodzeniem mechanicznym można stosować rury stalowe, rury z tworzyw sztucznych wzmocnione, korytka.

1. **SPECYFIKACJA**
	1. **WYMAGANIA W ZAKRESIE BEZPIECZEŃSTWA**

Strefy bezpieczeństwa - przyjęto podział obiektu na trzy strefy bezpieczeństwa:

* zewnętrzną
* ogólną
* specjalną

**Strefa zewnętrzna**

Strefę zewnętrzną tworzy bezpośrednie otoczenie budynku, dojścia i drogi dojazdowe, granicę strefy tworzą zewnętrzne ściany budynku wraz z drogami i chodnikami, które łączą budynek z otoczeniem. W strefie mogą występować zagrożenia takie jak:

* przestępstwa o charakterze chuligańskim
* napady rabunkowe
* kradzieże pojazdów
* kradzieże z włamaniem do pojazdów
* akty terroru skierowane przeciwko pracownikom budynku, oraz osobom czasowo przebywającym na terenie budynku

**Przewiduje się ochronę strefy poprzez:**

* System Telewizji Dozorowej (CCTV), który pozwoli na zasygnalizowanie i zarchiwizowanie (w celu ewentualnego wykorzystania w procesie dochodzeniowym i dowodowym) zaistniałych czynów o charakterze przestępczym.

**Strefa ogólna**

Strefa ogólna obejmuje swoim zasięgiem budynek od wejść poprzez poziome i pionowe drogi komunikacyjne (korytarze, klatki schodowe, dźwig osobowy), pomieszczenia użytkowe, techniczne, których zakłócenie pracy nie spowoduje nieodwracalnych strat dla całego budynku. W strefie mogą występować poniższe zagrożenia:

* zagrożenie napadem
* zagrożenie włamaniem (poprzez otwory drzwiowe i okienne)
* zagrożenie kradzieżą
* zagrożeniem aktami terroru, szantażu, wymuszeń
* zagrożeniem podpału lub pożaru

Przewiduje się ochronę strefy poprzez:

* System Sygnalizacji Włamania i Napadu (SSWiN)
* System Telewizji Dozorowej (CCTV)
* System Kontroli Dostępu (SKD)
* System Sygnalizacji Pożaru (SSP).

**Strefa specjalna**

Strefa specjalna obejmuje swoim zasięgiem część pomieszczeń mających wyjątkowe znaczenie dla:

* bezpieczeństwa budynku
* bezpieczeństwa działania jednostek zlokalizowanych w obiekcie
* bezpieczeństwa danych elektronicznych
* bezpieczeństwa przebywających w pomieszczeniach osób
* zagrożeniem podpału lub pożaru.

W tej grupie pomieszczeń znajdują się pomieszczenia: kontroli systemów, serwery, pomieszczenia UPS, rozdzielni piętrowych, w których znajdują się szafy kablowe okablowania strukturalnego, rozdzielnie RTE.

W strefie mogą występować zagrożenia o charakterze:

* komputerowo – informatycznym
* ekonomiczno-finansowym,

Przewiduje się ochronę strefy poprzez:

* System Sygnalizacji Włamania i Napadu (SSWiN)
* System Telewizji Dozorowej (CCTV)
* System Kontroli Dostępu (SKD)
* System Sygnalizacji Pożaru (SSP).

Systemy te mają zapewnić:

* pełną kontrolę ruchu osób, zarówno pracowników, interesantów jak i osób czasowo przebywających w budynku poza ustalonymi godzinami pracy
* zabezpieczenie antynapadowe i antywłamaniowe pomieszczeń z zastosowaniem indywidualnych stref uruchamianych przez odpowiedzialne za bezpieczeństwo wydzielonych pomieszczeń osoby
* pełny nadzór i rejestrację zdarzeń poprzez System Telewizji Dozorowej

## **SYSTEM TELEWIZJI DOZOROWEJ (CCTV)**

## **Założenia systemu**

Z uwagi na bezpośrednie sąsiedztwo budynku z przestrzenia publiczną – ulice w zarządzie miasta Rzeszowa, istnieje konieczność pełnego monitorowania otoczenia zewnętrznego kompleksu budynku. Biorąc pod uwagę wymienione zagrożenia dla poszczególnych stref należy przyjąć następującą koncepcję zabezpieczenie obiektu systemem monitoringu wizyjnego.

Dla Systemu Telewizji Dozorowej będzie to rejestracja wszelkich zjawisk zachodzących na terenie budynku (w miejscach objętych jego działaniem) przez 24 godziny na dobę. Zakłada się pełne monitorowanie otoczenia zewnętrznego budynku, wejść oraz miejsca parkowania przy budynku.

Monitoring wewnątrz budynku obejmuje ciągi komunikacyjne oraz pomieszczenia zgodnie z kartami technologicznymi.

Mając na uwadze rozległość strukturalną zabezpieczanego obiektu, planuje się dostawę systemu monitoringu wizyjnego opartego o sieć strukturalną TCP/IP. Rozwiązanie to charakteryzuję się elastyczną strukturą, bezstratną transmisją sygnałów i dużą odpornością na zakłócenia elektromagnetyczne.

System CCTV powinien być zaprojektowany w technologii IP. System będzie zarządzany z otwartego i w pełni skalowalnego systemu składającego się z serwera sieciowego umożliwiającego pracę w strukturze Serwer-Klient. Serwer rejestrujący powinien umożliwiać rejestrację co najmniej kilkudziesięciu sygnałów IP w jakości zapewniającej bezproblemową identyfikację osób.

* 1. **Oprogramowanie rejestrujące powinno**:
* umożliwiać instalację modułu Serwer i Klient jednocześnie na jednej stacji roboczej
* umożliwiać podgląd strumieni w formatach m.in: MJPEG, H.264, H.264+, H.265, H.265+ w rozdzielczości od 360x288 (CIF) do 4000x3000 (12M) i z prędkością odświeżania od 1 do 30 kl/s
* umożliwiać indywidulane ustawienia czasu rejestracji każdej z kamer
* umożliwiać pracę operatorowi w oparciu o minimum 3 niezależnie konfigurowanych monitorów dowolnej rozdzielczości
* nie zawierać licencji na kamery IP serwery i stacje operatorskie
* zawierać bezpłatne aktualizacje dostępne na stronie producenta
* powinno być kompatybilne w tył i w przód z produktami wybranego producenta
* system CCTV powinna charakteryzować min. 3 letnia gwarancja producenta.

System musi umożliwiać podłączanie kamer IP zgodnych ze standardem ONVIF.

System powinien umożliwiać nagrywanie obrazu oraz jednoczesny podgląd obrazu z wszystkich kamer. Wyświetlenie obrazu powinno się odbywać w podziale m.in.:

1x1; 1x2; 2x1; 2x2; 3x1; 3x2; 3x3; 3x4; 4x1; 4x2; 4x3; 4x4; 5x3; 5x4; 5x5; 6x4; 6x6; 6x7 7x4; 1+3; 1+5; 1+7; 1+8; 1+9; 1+12; 1+16; 1+1+2; 1+2+2; 1+1+4; 1+2+4 (dwa rodzaje); 1+4+4 (dwa rodzaje); 2+8; 4+9; 4+2+4 w trybie serwer-klient.

W pomieszczeniu monitorującym przewiduje się montaż stacji klienckiej zarządzającej i nadzorującej system bezpieczeństwa CCTV.

System CCTV oparty o w/w architekturę pozwala na praktycznie nieograniczoną swobodę w ewentualnej rozbudowie. Stanowisko operatorskie (stacje robocze) może znajdować się w każdym, dowolnie wybranym miejscu. Na stanowisko operatorskie składa się komputer z systemem Windows 10 IoT z podłączonym monitorem, mysz, klawiaturę. Dodatkowo, każde stanowisko robocze może zostać rozbudowane o dodatkowe monitory Należy zapewnić możliwość wyświetlania obrazów „ na żywo” oraz odtwarzanie danych archiwalnych na minimum 5-ciu oddzielnie konfigurowalnych monitorach jednocześnie.

System powinien umożliwiać zrealizowanie funkcji automatycznego powiadamiania operatorów systemu (ochrony) o fakcie np. pozostawienia obiektu bez nadzoru w danym miejscu, zaniku obrazu z kamery i nieautoryzowanych próbach manipulacji kamerą. A także pozwalać na reakcję po wykryciu zdarzenia poprzez: wysłanie zdjęcia na serwer FTP, wysłanie e-maila z powiadomieniem, wysterowania złącz alarmowych, czy pojawienia się komunikatu typu pop-up.

Do podglądu obrazów przesyłanych przez sieć może być wykorzystany komputer osobisty PC wyposażony w bezpłatne oprogramowanie zarządzające pracą kamer.

System będzie powiązany z systemem kontroli dostępu i sygnalizacji obecności. Informacje alarmowe z tych systemów będą skorelowane z pracą systemu CCTV. Integracja systemów pozwoli służbom ochrony na sprawniejszą ocenę zagrożeń i szybsze podejmowanie decyzji.

Zamontowany system będzie uzupełnieniem zaplanowanych w budynku systemów zabezpieczeń realizowanych na podstawie zintegrowanego systemu zarządzania budynkiem BMS. Zamontowany system monitoringu wizyjnego winien być zintegrowany z systemami zabezpieczeń KD, SAP poprzez protokół sieciowy TCP/IP i dedykowane oprogramowanie zarządzające systemami bezpieczeństwa.

W budynku w pomieszczeniu technicznym należy zainstalować serwer rejestrujący, który zostanie połączony z wykorzystaniem infrastruktury światłowodowej sieci LAN z centrum monitoringu Jednostki cyfrowe analizowałaby i rejestrowały obraz z kamer, znajdujących się na zewnątrz oraz wewnątrz obiektu. Na etapie projektu budowlanego należy ustalić miejsce rejestratora.

## **Urządzenia - Minimalne wymagania dla kamer**

Ze względu na specyfikę obiektów projektuje się system złożony z dwóch typów kamer tj.: kamera kopułowa oraz tubowa w rozdzielczościach odpowiednio dobranych do miejsca instalacji nie mniejszych niż 4 MPx. Kamery muszą posiadać wbudowany promiennik podczerwieni. Rozdzielczość kamery nie powinna być mniejsza niż 0,005lx/F1.6 w trybie kolorowym. Kamery muszą posiadać wbudowaną analitykę obrazu w postaci zliczania obiektów.

**Kamera IP wandaloodporna o stopniu ochrony IK10 na zewnątrz**

* Przetwornik – 4 MPX, 1/3”, SmartSens
* Rozdzielczość - 2688 (H) x 1520 (V)
* Czułość – nie gorsza niż 0.005 lx/F1.6 - tryb kolorowy
* Ogniskowa obiektu: f:2,8mm / F1.6
* Kompresja - H.265+, H.264+, MJPEG
* Interfejs – Ethernet
* Zasilanie – PoE, 12 VDC
* Klasa szczelności - IP67
* Oświetlacz podczerwieni: min. 45m
* Pobór mocy nie więcej niż 9 W przy włączonym IR

**Kamera IP wandaloodporna do wewnątrz**

* Przetwornik – 4 MPX, 1/3”, SmartSens
* Rozdzielczość – 2688 (H) x 1520 (V)
* Ogniskowa obiektu: f:2.8 mm/ F1.6
* Czułość – nie gorsza niż 0.005 lx/F1.6 - tryb kolorowy
* Kompresja – H.264+, H.265+, MJPEG
* Interfejs – Ethernet
* Zasilanie – PoE, 12 VDC
* Klasa szczelności – min.IP66
* Oświetlacz podczerwieni: min. 25m
* Pobór mocy nie więcej niż 7 W przy włączonym IR

|  |
| --- |
|  |

**Rozmieszczenie kamer**

* Kamery zewnętrzne:

Kamery należy rozmieścić w sposób umożliwiający obserwacją obiektów znajdujących się w odległości od kilku do kilkudziesięciu metrów od kamery, dla zapewnienia optymalnej możliwości rozróżniania szczegółów obrazu. Kamery zewnętrzne powinny umożliwiać obserwację obwodową budynku oraz terenu między budynkami.

* Kamery wewnętrzne winny być zamontowane w korytarzu obserwacja wejścia głównego oraz innych miejscach uznanych przez użytkownika za niezbędne

## **Serwer rejestrujący**

* Ilość kanałów IP – do 140 strumieni
* nagrywanie do 100 strumieni w rozdzielczości 1920x1080

 140 strumieni w rozdzielczości 1920x1080

* tryb nagrywania: ciągły, wyzwalany: ręcznie, wejściem alarmowym, detekcją ruchu, analiza obrazu
* Kompresja - H.264, H.264+, H.265, H.265+, MJPEG
* System operacyjny: Microsoft Windows 10 IoT
* Ilość dysków -min. 6 x HDD
* Wspierane protokoły: m.in. ONVIF, ONVIF fisheye, RTSP, RTSP fisheye, Novus, itp.

**Stacja operatorska**

* Dla kamer 4mpxwyświetlanie do: 40 strumieni pomocniczych lub do 7 strumieni głównych

odtwarzanie do: 7 strumieni głównych

* Wyszukiwanie nagrań: wg czasu/daty, powiązanych ze zdarzeniami, powiązanych z ciągiem znaków
* Metoda kopiowania nagrań: port USB (dysk twardy lub pamięć Flash), sieć komputerowa
* Obsługiwane protokoły: m.in. HTTP, TCP/IP, IPv4/v6, UDP, HTTPS, FTP, DHCP, DNS, RTSP, UPnP, SNM
* System operacyjny: Microsoft Windows 10 IoT
* Obsługa min 3 monitorów LCD.

Możliwość zarządzania przez urządzenia mobilne Android, IOS bez dodatkowych opłat.

System powinien oferować opcje automatycznego i względnie szybkiego tworzenia kopi zapasowych, aby zagwarantować długoterminowe archiwizowanie odpowiednich sekwencji obrazów i dźwięku.

Konfiguracja tworzenia kopii zapasowych powinna pozwolić użytkownikowi wskazywać różne katalogi dla przechowywania kopii zapasowych na nośnikach magazynujących połączonych lokalnie lub poprzez sieć, dla różnych zdarzeń dotyczących tworzenia kopii zapasowych. Ograniczeniem archiwizowanych nagrań powinna być tylko pojemność nośników pamięci oraz ich prędkość przetwarzania.

System musi dokonywać sprawdzania integralności nagrań, w celu eliminacji nieuprawnionej modyfikacji materiału video.

**Okablowanie**

## Kable muszą mieć opis umożliwiający ich identyfikacje w przypadku awarii. Opis na kablu należy umieścić z obydwu końców oraz na odejściu kabli na poszczególnych kondygnacjach jak również w miejscu wyjścia z budynku.

## W budynku okablowanie sygnałowe telewizji dozorowej należy prowadzić podtynkowo lub w korytach instalacji słaboprądowych zgodnie z wytycznymi okablowania dla sieci LAN .

# SYSTEM KONTROLI DOSTĘPU (SKD)

## **Uwagi ogólne**

## Celem zapewnienia optymalnych warunków bezpieczeństwa budynku, nadzorem będą objęte wszystkie drzwi pozwalające na wejście do budynku i do pomieszczeń wymagających specjalnej ochrony (strefa ogólna), oraz do przestrzeni wewnętrznych istotnych dla bezpieczeństwa pracy budynku (strefa specjalna).

## Podobnie jak system SSWIN, również system kontroli dostępu powinien być zintegrowany z systemem integracji i wizualizacji systemów bezpieczeństwa. Taka integracja znacząco zwiększy funkcjonalność integrowanych systemów, umożliwiając operatorowi systemów bezpieczeństwa identyfikację osób dokonujących zbrojenia systemu, nadawanie uprawnień z poziomu stacji operatorskiej, automatyczny proces zbrojenia systemu SSWIN, pełny monitoring przejścia nadzorowanego, w przypadku naruszenia strefy, zagrożenia pożarowego szybkiej identyfikacji miejsca zdarzenia, poprzez wyświetlenie obrazów z okolicznych kamer.

* Bezpośrednie współdziałanie systemu kontroli dostępu i systemu sygnalizacji włamania i napadu umożliwia wykorzystywanie czytników kart dostępu do uzbrajania i rozbrajania stref ochrony obejmujących zarówno pojedyncze pomieszczenia, jak i grupy pomieszczeń.
* Wszystkie drzwi objęte systemem sterowania powinny realizować funkcję wyjść ewakuacyjnych, oznacza to, że w przypadku sygnału z centralki pożarowej lub zadziałania wyłącznika awaryjnego otwarcia drzwi, rygle lub zaczepy zostaną automatycznie zwolnione.
* Wszystkie drzwi objęte systemem kontroli dostępu należy wyposażyć w magnetyczne czujniki otwarcia. Czujniki te winny być niezależne od czujników otwarcia zaczepu lub rygla. Ta niezależność, kontrolowana przez system, umożliwia rozróżnienie stanu normalnego lub nieautoryzowanego (inwazyjnego) otwarcia drzwi, umożliwia uruchomienie procedur alarmowych.
* System kontroli dostępu ma na celu ograniczenie i kontrolowanie ruchu osób w obiekcie lub na terenie objętym jego działaniem. Jest to realizowane poprzez przydzielanie prawa dostępu do chronionych przejść, pomieszczeń i obszarów osobom wyposażonym w elektroniczny identyfikator.
* System kontroli dostępu automatycznie rejestruje ruch każdej z osób i zapisuje związane z tym zdarzenia do archiwum zdarzeń na dysku komputera.
* Ze względu na specyfikę obiektu proponowany system powinien spełniać wymienione w dalszych punktach szczegółowe wymagania. Wymagania te dotyczą zarówno parametrów technicznych i konstrukcyjnych urządzeń jak również możliwych do zrealizowania funkcji użytkowych. Proponowany system powinien być bardzo elastyczny, umożliwiać łatwą rozbudowę oraz nie wnosić istotnych ograniczeń ilościowych pod względem ilości kontrolowanych przejść i liczby użytkowników. Jest to istotne ze względu na planowaną rozbudowę rozproszonego systemu obejmującego wiele lokalizacji.

**Wymagania do kontrolera SKD**

Kontroler SKD musi być dedykowany do oprogramowania integracji i wizualizacji, umożliwiający identyfikację użytkowników przy pomocy kart typu Unique, Mifare Classic, Mifare Desfire.

**Porty do czytników 2**

**Liczba drzwi dwustronnych 1**

**Liczba drzwi jednostronnych 2**

**Port czytnika Wiegand**

**Porty komunikacyjne TCP**

**Pamięć kart 20 000**

**Pamięć zdarzeń 50 000**

**Liczba linii dozorowych 6**

**Liczba wyjść sterujących 3**

**Zasilanie kontrolera 12 VDC**

**Zasilanie z akumulatora 12 V / 7 Ah**

**Zakres temperatur -10°C do 55°C**

**Wilgotność (bez kondensacji) 10% - 90%**

**Typy czytników zbliżeniowe, magnetyczne, biometryczne**

**Wyjścia do czytników 12V**

**Typ przewodu/maksymalna długość do czujnika na końcu linii AWG #22 - 300 m**

**Wyjście zamka przekaźnikowe**

**Monitorowane wyjścia do zamków nie**

**Wyjścia sterujące do sygnalizatorów w czytnikach 4**

**Port rozszerzeń 1 x port modułu 4 przekaźników**

* 1. **SYSTEM REJESTRACJI CZASU PRACY (RCP)**

**Uwagi ogólne**

Systemy Rejestracji Czasu Pracy (RCP), to narzędzia pozwalające kontrolować i zarządzać wszystkimi zdarzeniami pracowniczymi w firmie. Zarówno wejściami, wyjściami, przerwami w pracy, jak i obecnościami lub nieobecnościami danego pracownika. Dla tego, aby lepiej i efektywniej rozliczać czas pracy całej załogi i naliczać wynagrodzenia. Systemy RCP automatyzują powtarzalne czynności, takie jak np. rozliczanie wyjść służbowych czy odliczanie od wynagrodzenia spóźnień.

Najczęściej podstawowy system RCP składa się z wydanych kart pracowniczych (identyfikatorów), a także czytników (urządzeń rejestrujących), które zamontowane są np. przy wejściu i wyjściu z danego zakładu. Zapis informacji odbywa się w momencie przyłożenia identyfikatora do czytnika. Dane przekazywane są do ogólnego systemu, dzięki specjalnemu oprogramowaniu. Tak tworzona jest cała elektroniczna dokumentacja danego pracownika.

Co więcej, sieć czytników rozlokowanych w halach czy biurach (często wyposażona np. w dodatkowe bramki obrotowe czy przejścia typu tripod), pozwala m.in. na:

* wyliczenie realnych wartości czasu pracy i nadgodzin – RCP pomaga poprawić dyscyplinę pracowników i zwiększa efektywność ich pracy
* ustalenie harmonogramów pracy dla grup pracowników – system pozwala planować czas pracy, także w systemie zmianowym
* nadzorowanie wejść i wyjść – RCP pomaga szybko i sprawnie zarejestrować swoją obecność w pracy
* rejestrowanie nieobecności (zwolnienia, spóźnienia) – system automatycznie nalicza absencje
* planowanie i rozliczanie urlopów – rejestrator pozwala złożyć wnioski o urlop czy wyjścia prywatne
* szczegółowe raportowanie wszystkich danych – RCP pozwala generować i drukować dowolne raporty z danymi dotyczącymi czasu pracy.

**Wymagania do kontrolera RCP**

Terminal rejestracji czasu pracy musi być dedykowany do oprogramowania integracji i wizualizacji, umożliwiający identyfikację użytkowników przy pomocy kart typu Unique, Mifare Classic, Mifare Desfire.

**Liczba kart 50 tys.**

**Bufor zdarzeń 150 tys.**

**Liczba przycisków funkcyjnych 8**

**Wyświetlacz kolorowy Kolorowy**

**Typ wbudowanego czytnika kart Unique (125 kHz), Mifare Classic(13,56 MHz), Mifare Desfire (13,56 MHz)**

**Identyfikacja biometryczna Nie**

**Sterowanie zamkiem Tak**

**Wymiary 205,6 x 150 x 41,6**

**Zasilanie 12 V DC**

**Porty komunikacyjne TCP/IP, USB**

**Funkcjonalności kod pracy, czas letni/zimowy, programowany dzwonek, wpisywanie tekstu metodą T9, identyfikator ze zdjęciem, 9-cyfrowy identyfikator użytkownika, funkcja anti-passback**.

**Temperatura pracy 0°C do +45°C**

* 1. **PARAMETRY TECHNICZNE I KONSTRUKCYJNE SYSTEMU INTEGRACYJNEGO:**

Informacje ogólne

Pod względem parametrów technicznych proponowane urządzenia spełniają wyszczególnione poniżej założenia:

Urządzenia i oprogramowanie wchodzące w skład systemu pod względem jakościowymi funkcjonalnym powinny spełniać wymagania zawarte w punkcie 12 – klasa S1, S2, S3 lub S4 PN-EN-60839-11-1 Część 11-1: Elektroniczne systemy kontroli dostępu.

* 1. Wymagania dotyczące systemów i części składowych:
* Urządzenia identyfikujące użytkownika – karty zbliżeniowe i czytniki o zróżnicowanym zasięgu odczytu.
* Karty (elektroniczne identyfikatory) posiadają zakodowany w procesie produkcji unikatowy numer seryjny oraz możliwość personalizacji.
* Sterowniki (kontrolery) współpracujące z czytnikami oraz z pozostałymi elementami (zamki elektryczne, przyciski, czujniki stanu drzwi itp.) powinny posiadać możliwość pracy w trybie komunikacji z programem nadzorczym i autonomicznym oraz przy zaniku podstawowego zasilania sieciowego (230VAC). Praca w trybie autonomicznym powinna zapewniać zachowanie uprawnień w zakresie dostępu dla użytkowników (min 18 000 kart, gwarantować zapis, co najmniej 48 000 ostatnich zdarzeń oraz pozostałych parametrów związanych z działaniem kontrolowanego przejścia.
* Po zaniku podstawowego zasilania sieciowego sterownik powinien automatycznie przełączyć się na pracę z zasilania awaryjnego (akumulator) i pracować, co najmniej przez 8 godzin. System powinien sygnalizować stan dołączonych do sterowników akumulatorów pod względem ich pełnego naładowania. Sterownik powinien automatycznie wyłączać się po osiągnięciu przez akumulator najniższego dopuszczalnego poziomu napięcia a następnie automatycznie wznawiać pracę po przywróceniu podstawowego zasilania sieciowego.
* Aby zagwarantować odpowiednie bezpieczeństwo i niezawodność działania systemu w skali całego obiektu, system powinien oferować sterownik obsługujący jedno przejście w wersji z jednym lub dwoma czytnikami. Takie rozwiązanie gwarantuje, że w przypadku awarii jednego sterownika tylko jedno przejście będzie wyłączone a pozostałe będą pracowały poprawnie. Gdy kontrolowane przejścia są zlokalizowane w pobliżu dopuszcza się sterowniki obsługujące dwa lub cztery przejścia. Uszkodzenie sterownika lub obwodu zamka elektrycznego musi być bezwzględnie sygnalizowane na stacji monitorującej odpowiednim komunikatem alarmowym i sygnałem dźwiękowym.
* System powinien mieć możliwość zastosowania sterowników kontroli dostępu współpracujących z modułami rozszerzeń, które umożliwiają zwiększenie liczby wejść parametrycznych linii dozorowych oraz przekaźnikowych lub tranzystorowych wyjść sterujących dla zapewnienia współpracy z urządzeniami zewnętrznymi (np. windami).
* Obudowa sterownika powinna uniemożliwiać bezpośredni dostęp osobom nieuprawnionym a jej otwarcie w każdym przypadku powinno być sygnalizowane alarmem dla służb ochrony obiektu.
* Sterowniki w systemie powinny mieć możliwość komunikacji z komputerem i programem nadzorczym poprzez magistralę komunikacyjną z protokółem TCP/IP. Uszkodzenie magistrali lub utrata komunikacji z kontrolerem powinno być sygnalizowane alarmem.
	1. **FUNKCJE SZCZEGÓŁOWE PROGRAMU NADZORCZEGO**

Program nadzorczy systemu kontroli dostępu powinien umożliwiać realizację następujących funkcji szczegółowych:

* wizualizacja stanu elementów systemu poprzez hierarchiczny zestaw map graficznych z animowanymi ikonami, których stan jest aktualizowany w czasie rzeczywistym;
* każda z ikon na mapie powinna posiadać menu kontekstowe umożliwiające wykonywanie określonych poleceń oraz wyświetlenie okna z kompletnym statusem elementu;
* informacje dotyczące wszelkiej aktywności w systemie wyświetlane w postaci komunikatów w oknie zdarzeń;
* możliwość personalizacji układu okien wyświetlanych na pulpicie operatora;
* uzupełnienie bazy o użytkowników o zdjęcia oraz możliwość ich wyświetlania na ekranie monitora po użyciu karty;
* automatyczne wyświetlanie okien wideo zawierających obrazy z kamer przypisanych do elementu w stanie alarmu;
* możliwość generowania filtrowanego raportów wprost z okna zdarzeń;
* możliwość generowania prostych raportów rejestracji czasu pracy pracowników w oparciu o te same karty i czytniki, które są używane w systemie kontroli dostępu;
* dostęp do wybranego pomieszczenia po użyciu ważnych kart przez dwóch użytkowników;
* uzbrajanie wybranych drzwi połączone z blokadą uprawnień dla pozostałych użytkowników;
* import /eksport plików z danymi użytkowników;
* funkcja kontroli dwustronnej „anti-passback” lokalny wymuszająca na użytkownikach konieczność używania kart na wejściu i wyjściu;
* realizację tzw. „śluzy”, czyli blokady dostępu do drzwi, jeżeli są otwarte drzwi następujące po nich;
* funkcja wielokrotnego odczytu karty (2 lub 3 kolejne odczyty) w celu realizacji zaprogramowanej sekwencji zdarzeń np. odryglowania/zaryglowania drzwi na stałe, uzbrojenia rozbrojenia centrali alarmowej, włączenia /wyłączenia oświetlenia lub klimatyzacji.

**Zasilanie systemu**

Kontrolery systemu należy zasilić napięciem 230VAC, przewodem typu YDY 3x1.5mm2 z obwodu w rozdzielni elektrycznej. Wszystkie urządzenia systemu posiadają wbudowane akumulatory zapewniające pracę pod odłączeniu zasilania podstawowego.

**Instalacje**

Połączenia kablowe systemu kontroli dostępu należy wykonać przewodami:

* Połączenie kontrolerów z magistralą U/UTP cat.5 4x2x0.5mm
* Podłączenie czytników zbliżeniowych U/UTP cat.5 4x2x0.5mm
* Podłączenie kontaktronu OWY 2x1 mm
* Podłączenie przycisku wyjścia YTDY 6x0.5 mm
* Podłączenie elektrozaczepy OMY 3X0.75mm

**Montaż urządzeń i instalacji**

System kontroli dostępu obejmować będzie wyznaczone przez przedstawicieli Inwestora wyjścia ewakuacyjne, przejścia jednostronne, przejścia jednostronne czasowo otwierane przez personel.

System będzie oparty na kontrolerach komunikujących się poprzez IP z serwerem systemu pracującym pod programem nadzorczym. Serwer umieścić w pomieszczeniach serwerowni, natomiast kontrolery rozmieszczać w pobliżu kontrolowanych przejść, z optymalnym wykorzystaniem ich zajętości, na terenie całego obiektu w czystych i niezapylonych miejscach zgodnie z rysunkami. O ile charakterystyka pomieszczeń na to pozwala, kontrolery należy instalować, na ścianach powyżej zasięgu ramion człowieka. Lokalizacje ,w których skupiono więcej niż jeden kontroler, należy łączyć z siecią IP. System zaprojektowano wykorzystując sieć IP.

**Elementy wchodzące w skład systemu:**

* **Czytnik kart zbliżeniowych**

Przeznaczony do pracy w systemach kontroli dostępu z możliwością montażu wewnątrz i na zewnątrz pomieszczeń. Posiadający obudowę z tworzywa ABS spełniającą wymagania normy IP66 (wodoodporność). Czytnik przeznaczony do współpracy z kontrolerami z interfejsem Wieganda. Urządzenie musi odczytywać Mifare Classic (13,56 MHz). Zasięg odczytu kart zbliżeniowych wynosi od 2 do 5 cm w zależności od rodzaju karty.

* **Kontrolery**

Należy zastosować kontrolery pracujące pod nadzorem dedykowanego oprogramowania nadzorczego. Kontrolery powinny posiadać 2-4 portów czytników, co umożliwia kontrolę do 4 drzwi jednostronnie. Wbudowana pamięć zdarzeń nie powinna być mniejsza niż 48 000, a pamięć kart nie mniejsza niż 18 000. Kontroler powinien zawierać liczbę wyjść sterujących nie mniejszą niż 4. Porty czytnika powinny pracować w oparciu o powszechną komunikację typu Wiegand. Porty komunikacyjne powinny łączyć się z oprogramowaniem nadzorczym poprzez protokół TCP/IP.

* **Program nadzorczy**

Program nadzorczy, dedykowany jest do współpracy z kontrolerami w trybie sieciowym.

Interfejs operatora musi umożliwiać:

* konfigurację parametrów fizycznych elementów systemu
* definiowanie elementów logicznych
* monitorowanie stanu systemu „on-line” poprzez system graficznych map obiektów i komunikatów
* wyświetlanie zdjęć użytkownika po użyciu karty
* generowanie filtrowanych raportów zdarzeń i zapis w formacie \*.xls
* dostęp po użyciu 2, 3 lub 4 kart
* pierwsze otwarcie kontrolowanego przejścia przez tzw. „pierwszą kartę” ze specjalnymi uprawnieniami
* dostęp po potwierdzeniu przez operatora.
* **Dodatkowo w skład systemu wchodzą:**
* Zasilacz buforowy wraz z obudową. Zasilanie 12 V 5A
* Przycisk wyjścia, styki NO/NC
* Przycisk wyjścia awaryjnego, 2 pary styków NO/NC
* Elektrozaczep niskoprądowy 12V
* Kontaktron systemu KD dopasowany do stolarki drzwiowej
* **Wizualizacja**

Wizualizacja systemu SAP i integracja systemów CCTV, KD, powinna być prezentowana na stacji operatorskiej systemu SMS budynku.

System musi posiadać wyspecjalizowany interfejs graficzny, pozwalający na szybką identyfikację i obsługę alarmów.

Poszczególne sytuacje mają być wyświetlane w sposób graficzny, z podpowiedziami algorytmów postępowania. Ekran obsługi zdarzeń w systemie ma zawierać listę zdarzeń, takich jak np. alarmy wymagające obsługi przez operatora. Zdarzenia mają być uporządkowane według kategorii ważności i wyświetlane w kolorze wskazującym rodzaj zdarzenia oraz status jego obsługi. Przeglądarka obiektów ma umożliwiać nawigację w obszarze wszystkich poziomów instalacji i zarządzanie wszystkimi skonfigurowanymi elementami.

Nawigacja ma odbywać się w strukturze hierarchicznej, odzwierciedlającej instalację oraz za pomocą map sytuacyjnych. Wizualizowane plany architektoniczne chronionego budynku muszą umożliwiać powiększenie obszaru w dowolnym jego fragmencie, wybór kondygnacji lub mapy z terenem zewnętrznym. Ponadto, podczas alarmu system wizualizacyjny powinien automatycznie przybliżyć i wskazać obszar zagrożenia służbom ochrony. Wizualizowane plany budynku muszą zawierać aktualny rozkład pomieszczeń według rzeczywistych aranżacji.

Możliwość włączenia komunikatów głosowych, dla łatwiejszej pracy operatora i tworzenia automatycznych scenariuszy np.:

* reakcją programu na alarm może być np. wyświetlenie obrazów z kamery CCTV w miejscu wystąpienia alarmu, zmiana aktywnego widoku lub uruchomienie zewnętrznej aplikacji
* w momencie alarmu w danej strefie dozorowej, wszystkie przejścia KD na drodze dojścia do strefy są otwarte na czas weryfikacji alarmu przez obsługę obiektu
* powiadamianie przez aplikację kliencką, e-mail, sms
* archiwum zdarzeń wszystkich systemów (CCTV, PPOŻ oraz KD). Dzięki temu operator zobaczy pełną historię alarmów, awarii, logowania użytkowników i może je łatwiej analizować. Zdarzenia można filtrować po dacie, rodzaju systemu, typie urządzeń i wielu innych, a całą bazę lub jej wybraną część można eksportować do pliku PDF
* możliwość integracji różnych systemów bezpieczeństwa z wykorzystaniem protokołu TCP/IP lub zarządzających budynkiem w oparciu o moduły sieciowe wejścia/wyjścia.
1. **KONTROLA JAKOŚCI PRAC**

Ogólne zasady kontroli jakości prac

Materiały posiadające atest producenta stwierdzający ich pełną zgodność z warunkami podanymi w specyfikacjach, mogą być przez Zamawiającego dopuszczone do użycia bez badań. Przed przystąpieniem do badania, Wykonawca powinien powiadomić Zamawiającego o rodzaju i terminie badania. Po wykonaniu badania, Wykonawca przedstawia na piśmie wyniki badań do akceptacji Zamawiającego. Wykonawca powiadamia pisemnie Zamawiającego o zakończeniu każdej pracy zanikającej, którą może kontynuować dopiero po stwierdzeniu przez Zamawiającego. Wszystkie elementy prac instalacji elektrycznych podlegają sprawdzeniu w zakresie: - zgodności z dokumentacją i przepisami; - zgodności materiałów z wymaganiami norm; - poprawności oznaczenia; - kompletności wyposażenia; - poprawności montażu; - braku widocznych uszkodzeń;- należytego stanu izolacji; - skuteczności ochrony od porażeń;

Badania przed przystąpieniem do prac, Wykonawca powinien uzyskać od producentów deklaracje zgodności i gdy to jest wymagane certyfikat na oznaczenie materiału znakiem CE. Na żądanie Zamawiającego, należy dokonać testowania sprzętu posiadającego możliwość nastawienia mechanizmów regulacyjnych. W wyniku badań testujących należy przedstawić Zamawiającego świadectwa cechowania.

1. **OBMIAR PRAC**

Obmiaru prac dokonać należy w oparciu o dokumentację powykonawczą i ewentualnie dodatkowe ustalenia, wynikłe w czasie realizacji przedmiotu zamówienia.

Odbiory prac przewidzianych do zakrycia: przewody do urządzeń montowanych w ścianach - odbiory elementów po próbach funkcjonalnych oddzielnie CCTV , SAP, KD i SSWIN.

Zasady odbioru końcowego

Odbioru robót dokonuje zespół powołany przez Zamawiającego, po całkowitym zakończeniu prac i dokonaniu prób funkcjonalnych. Przyjęcie prac może nastąpić tylko w przypadku pozytywnego wyniku przeprowadzonych prób i pomiarów, uzgodnieniami z Zamawiającym oraz obowiązującymi normami i przepisami. Wykonawca zobowiązany jest dostarczyć zamawiającemu następujące dokumenty:

* aktualną dokumentację powykonawczą
* protokoły z dokonanych pomiarów
1. **ZAKRES PRAC**
* inwentaryzację stanu istniejącego;
* kontrolą dostępu objąć wejścia z głównej klatki schodowej na ciągi korytarzy;
* na parterze przewidzieć ograniczenie dostępu przy pomocy dwustronnej bariery podczerwieni;
* kontrola dostępu dla windy osobowej – umożliwiająca jazdę tylko na wybrane piętro;
* zaprojektować stację roboczą dla systemu kontroli dostępu, wizualizacja i monitoring przejść, nadawanie i usuwanie uprawnień dla poszczególnych kart;
* należy zaprojektować system kontroli dostępu obsługujący min. 250 kart;
* istniejący system sygnalizacji pożaru przystosować do współpracy z projektowanym system kontroli dostępu – zwolnienie drzwi objętych kontrolą dostępu w razie wykrycia pożaru na drogach ewakuacyjnych;
* system monitoringu CCTV – ok. 17 kamer;
* stacje roboczą wraz z monitorem 32” do pracy ciągłej – na portierni;
* rozbudowa istniejącej rozdzielni piętrowej w zakresie niezbędnym do zasilania projektowanych urządzeń;
* zestawienie materiałów;

1. **ZESTAWIENIE SPRZĘTU OBJĘTEGO PRZEDMIOTEM ZAMÓWIENIA**

|  |  |  |
| --- | --- | --- |
| L.p. | Opis  | Liczba [szt.] |
| 1 | Program nadzorczy SKD: - Windows 7/8/10, - do 4096 kontrolowanych przejść - komunikacja z kontrolerami: TCP/IP lub RS485 - pełny monitoring stanów i wizualizacja elementów systemu na mapach, generator raportów RCP - wersje językowe oprogramowania: polska. | 1 |
| 2 | Kontroler standardowy; porty do czytników: 2; liczba drzwi dwustronnych: 1; liczba drzwi jednostronnych: 2; porty komunikacyjne: TCP; pamięć kart: 20 000; pamięć zdarzeń: 50 000; liczba linii dozorowych: 6; liczba wyjść sterujących: 3; zasilanie kontrolera: 12 VDC.  | 6 |
| 3 | Zasilacz buforowy typu przetwornica do kontrolera. Zasilanie 12V DC, 5 A. Do zasilania modułu kontrolera, czytników, zamków elektrycznych i ładowania akumulatora 7 Ah. | 6 |
| 4 | Akumulator bezobsługowy 7Ah/12V; wymiary (wys. x szer. x gł.): 94+6 x 151 x 65mm; napięcie ładowania [25°C]: praca buforowa: od 13.38 V do 13.8 V (-20mV°C), praca cykliczna: od 14.4 V do 14.7 V (-30mV°C); maks. prąd ładowania: 2.8A.  | 6 |
| 5 | Czytnik administratora; standard kart: MIFARE®; częstotliwość pracy: 13,56 MHz; zasięg odczytu: do 5 cm; interfejs wyjściowy: USB; kolor: czarny; wymiary: 106 mm x 82 mm x 25 mm.  | 1 |
| 6 | Czytnik kart zbliżeniowych; standard kart: MIFARE®; częstotliwość pracy: 13,56 MHz; zasięg odczytu: do 5 cm; interfejs wyjściowy: Wiegand; typ złącza: kabel elastyczny; kolor: czarny; wymiary: 120 mm x 48 mm x 20 mm.  | 11 |
| 7 | Karta zbliżeniowa; rodzaj: karta ISO; format: kompatybilny z MIFARE®; częstotliwość pracy: 13,56 MHz; do nadruku.  | 250 |
| 8 | Przycisk wyjścia; styki: NC / NO / C; wymiary: 70 x 70 x 34 mm; typ montażu: nawierzchniowy; zakres temperatur: od -10°C do 55°C; obciążalność: 5A / 125VAC.  | 8 |
| 9 | Przycisk wyjścia awaryjnego; styki: 2 pary zacisków C / NO / NC; wymiary: 87 x 87 x 58 mm; typ montażu: nawierzchniowy; zakres temperatur: od -30°C do 70°C; Obciążalność: 2A 30VDC.  | 8 |
| 10 | Czujka magnetyczna Grade 2 ; parametry kontaktronu: 0.5A/100VDC/10W/200mΩ; Styk: NC; zastosowanie: okna, drzwi drewniane; stopień zabezpieczenia: Grade II (stopień 2); pętla sabotażowa: tak; wyprowadzenie: kablowe (przewód 35 cm); odległość zadziałania: 15mm - 25mm; kolor: brązowy; wymiary: kontaktron: 17.5mm x 9mm (DŁxŚR), magnes: 17.5mm x 9mm (DŁxŚR).  | 8 |
| 11 | Elektrozaczep; rodzaj zamka: bez zasilania otwarty (NO); pobór prądu: 190 mA; zasilanie: 12V DC; wymiary (mm): 75 x 20.5 x 28.5;  | 8 |
| 12 | Licencja; 1 punkt RCP (kontroler lub terminal).Włącza funkcjonalność RCP i 1 punkt RCP. | 1 |
| 13 | Terminal Rejestracji Czasu Pracy i Kontroli Dostępu; liczba kart: 50 000; bufor zdarzeń: 150 000; liczb przycisków funkcyjnych: 8; wyświetlacz: kolorowy; typ wbudowanego czytnika kart: Unique (125 kHz), Mifare Classic(13,56 MHz), Mifare Desfire (13,56 MHz); sterowanie zamkiem: tak; zasilanie: 12 V DC; porty komunikacyjne: TCP/IP, USB.  | 1 |
| 14 | Zasilacz buforowy 13,8V/2,6A + styki sabotaż., dla AKU 7Ah. | 1 |
| 15 | Akumulator bezobsługowy 7Ah/12V; wymiary (wys. x szer. x gł.): 94+6 x 151 x 65mm; napięcie ładowania [25°C]: praca buforowa: od 13.38 V do 13.8 V (-20mV°C), praca cykliczna: od 14.4 V do 14.7 V (-30mV°C); maks. prąd ładowania: 2.8A. | 1 |
| 16 | Kamera IP z analizą obrazu w oparciu o Deep Learning; 4 MPX, CMOS 1/3” SmartSens; DSS; WDR (podwójne skanowanie przetwornika), 120dB; DNR: 2D, 3D; Defog (F-DNR); HLC; obiektyw: f=2.8 mm/F1.6; mechaniczny filtr podczerwieni; 30 kl/s dla 2592 x 1520, 60 kl/s dla 1920 x 1080 (Full HD) i niższych rozdzielczości; liczba strumieni: 3; kompresja: H.264, H.264+, H.265, H.265+, MJPEG; strefy prywatności: 4; detekcja ruchu; funkcje analizy obrazu: sabotaż, pozostawienie obiektu, zniknięcie obiektu, przekroczenie linii, wkroczenie do strefy, wyjście ze strefy, zliczanie obiektów, detekcja twarzy, detekcja osób, detekcja osób nienoszących maski, zliczanie przekroczeń linii, mapa ciepła, zmiana sceny, utrata ostrości, zmiana kolorystyki, rozróżnianie obiektów, zliczanie osób, zliczanie pojazdów, wtargnięcie; zasięg IR do 30 m; wej./wyj. audio wbudowany mikrofon; obsługa kart: microSD; średnica: 94 mm; obudowa: IP 67; obudowa: wandaloodporna IK10, aluminiowa, w kolorze białym; zasilanie: PoE, 12 VDC; temp. pracy: -30°C ~ 60°C.  | 17 |
| 17 | Adapter ścienny/sufitowy, wewnętrzny/zewnętrzny; wykonanie: aluminium; kolor biały; IP 66; wymiary (mm): 140 φ x 50 (wysokość). | 17 |
| 18 | 18 Port managed CCTV PoE switch, long range, 250W (1 year NCC Pro pack license bundled). | 2 |
| 19 | Rejestrator IP; do 140 kanałów wideo i audio; łączna przepustowość nagrywania 350 Mbit/s; prędkość nagrywania do 3500kl/s;prędkość wyświetlania do 1050kl/s;obsługa do 6 x HDD; obsługa rozdzielczości 4000 x 3000 i niższych; do 3 monitorów jednocześnie; System operacyjny: Microsoft Windows 10 IoT; możliwość współpracy z zewnętrznymi macierzami dyskowymi;możliwość instalacji w szafie RACK (obudowa: 4U). | 1 |
| 20 | Dysk twardy 8TB (interfejs SATA. dedykowany do pracy 24/7) z instalacją i testowaniem | 2 |
| 21 | Stacja kliencka CCTV; Kamery IP: do 42 kanałów w rozdzielczości 640 x 480 wykorzystując kodek H.264 (wideo + audio), do 30 kanałów w rozdzielczości 640 x 480 wykorzystując kodek H.265 (wideo + audio); do 3 monitorów jednocześnie; System operacyjny: Microsoft Windows 10 IoT. | 1 |
| 22 | Oprogramowanie do wizualizacji i integracji systemów zabezpieczenia mienia; Integrowane systemy: CCTV, SSP, SSWIN, SKD; Ograniczenie ilości elementów: 1000; Liczba obsługiwanych stacji klienckich: 4; Liczba obsługiwanych paneli: bez ograniczeń; Liczba obsługiwanych scenariuszy: bez ograniczeń | 1 |
| 23 | Dedykowana stacja kliencka do wizualizacji i integracji systemów zabezpieczenia mienia z zainstalowanym oprogramowaniem, obsługa do 6 monitorów jednocześnie. | 1 |
| 24 | Dedykowany serwer z zainstalowanym oprogramowaniem do wizualizacji i integracji systemów zabezpieczenia mienia, obsługa do 3 monitorów jednocześnie, możliwość instalacji w szafie RACK (obudowa 19"; 4U). | 1 |
| 25 | Monitor; Matryca: IPS podświetlenie LED; przekątna ekranu: 31.5"; rozdzielczość matrycy: 1920 x 1080; format: 16:9; jasność: 300 cd/m2; kontrast: 20000000:1; czas odpowiedzi matrycy: 5 ms; wbudowane głośniki: 2 x 3 W; wejścia wideo: 1 x CVBS, złącze BNC (przelotowe) 1 x VGA 1 x HDMI 1 x DVI; wejścia audio: 1 x Mini Jack stereo, 1 x Mini Jack stereo; złącze multimedialne: USB 2.0; zasilanie: 100 ~ 240 VAC; standard mocowania: VESA 100 x 100 mm; przystosowany do pracy ciągłej (24/7); przystosowany do pracy ciągłej (24/7); podświetlenie LED; funkcja zapobiegająca „wypalaniu” statycznego obrazu na matrycy. | 2 |
| 26 | Automatyczne bramki uchylne wyposażone w mechanizm dwukierunkowy oraz piktogramy informacyjne. Wymiary: średnica korpusu bramek: max. 130 mm, długość ramion min. 400 mm, wysokość ramion od 600 mm do 700 mm. Wykonanie: obudowa korpusu ze stali nierdzewnej, ramiona bramek szkło hartowane przeźroczyste/mleczne o gr. min. 9 mm. | 4 |