

PROGRAM FUNKCJONALNO- UŻYTKOWY (PFU)

Dla zadania inwestycyjnego realizowanego w formule „Zaprojektuj i Wybuduj”

NAZWA ZADANIA:

„Modernizacja i przebudowa systemu kontroli dostępu i monitoringu wizyjnego w budynku prokuratur poznańskich przy ul. Solnej 10 w Poznaniu”

Adres obiektu budowlanego: ul. Solna 10, 61-736 Poznań

Wspólny Słownik Zamówień (Kody CPV): Zamówienie klasyfikowane jest zgodnie ze Wspólnym Słownikiem Zamówień za pomocą następujących kodów:

- **42961100-1** – Systemy kontroli dostępu
- **32323500-8** – Urządzenia do nadzoru wideo
- **71320000-7** – Usługi inżynierskie w zakresie projektowania
- **51312000-2** – Usługi instalowania urządzeń radiowych, telewizyjnych, dźwiękowych i wideo

Nazwa i adres zamawiającego:

Prokuratura Okręgowa w Poznaniu, ul. Solna 10, 61-736 Poznań

Opracował: Marcin Adamczyk

Spis zawartości programu funkcjonalno-użytkowego

- I. **Część opisowa.**
 - 1. **Opis ogólny przedmiotu zamówienia.**
 - 1.1 Zakres robót budowlanych.
 - 1.2 Uwarunkowania wykonania przedmiotu zamówienia.
 - 1.3 Ogólne właściwości funkcjonalno-użytkowe.
 - 2. **Opis wymagań zamawiającego w stosunku do przedmiotu zamówienia.**
- II. **Część informacyjna.**

CZĘŚĆ I:

1. OPIS OGÓLNY PRZEDMIOTU ZAMÓWIENIA

Przedmiot i cel inwestycji

Przedmiotem zamówienia jest opracowanie pełnej wielobranżowej dokumentacji projektowej (w tym projektu wykonawczego i technicznego), a następnie kompleksowe wykonanie robót instalacyjno-budowlanych w formule „**Zaprojektuj i Wybuduj**”. Inwestycja obejmuje całkowity demontaż wyeksploatowanych, przestarzałych systemów bezpieczeństwa technicznego oraz wdrożenie nowoczesnego, cyfrowego, zintegrowanego systemu kontroli dostępu (SKD) i telewizji dozorowej IP (VSS/CCTV) wraz z niezbędną infrastrukturą sieciowo-szkieletową i serwerową w budynku Prokuratury poznańskich przy ul. Solnej 10.

Głównym celem zadania jest podniesienie poziomu bezpieczeństwa technicznego, operacyjnego i cybernetycznego obiektu o zaostrzonym rygorze dostępu, przy jednoczesnym zapewnieniu pełnej zgodności z Krajowym Systemem Cyberbezpieczeństwa (KSC), unijną dyrektywą NIS2, dyrektywą CER oraz wymogami RODO.

1.1 Zakres robót budowlanych

Zakres robót budowlanych i instalacyjnych obejmuje **modernizację i przebudowę systemu kontroli dostępu i monitoringu wizyjnego w budynku prokuratury poznańskich przy ul. Solnej 10 w Poznaniu**. Zakres robót obejmuje:

1. Prace demontażowe (Wymiana istniejącego systemu)

- Demontaż starych kamer zewnętrznych: 16 sztuk.
- Demontaż starych kamer wewnętrznych: Łącznie 70 sztuk (10 sztuk w roku 2026 oraz 60 sztuk w roku 2027).

2. Instalację i montaż urządzeń systemu telewizji dozorowej (CCTV):

- Montaż kamer zewnętrznych: 16 sztuk, w tym:
 - 8 kamer szybkoobrotowych PTZ (5MP IP, z oświetlaczem IR) montowanych na uchwytych ściennych i adapterach słupowych.
 - 8 kamer tubowych (8 MP, z obiektywem Moto-Zoom) wraz z puszkami połączeniowymi i adapterami słupowymi.
- Montaż kamer wewnętrznych: 70 kamer kopułowych IP (5 MP z obiektywem Moto-Zoom) wraz z dedykowanymi puszkami połączeniowymi (10 sztuk w 2026 r. i 60 sztuk w 2027 r.).
- Montaż torów transmisyjnych: 70 zestawów aktywnych konwerterów do transmisji sygnału Ethernet oraz zasilania PoE po istniejących kablach koncentrycznych.

3. Budowę i konfigurację centrum nadzoru oraz infrastruktury IT

- **Montaż urządzeń w serwerowni:**
 - Instalacja 2 szaf dystrybucyjnych Rack 19" o gabarytach od 33U do 48U wraz z wyposażeniem.
 - Montaż 2 serwerów Dell PowerEdge R360 (procesor Xeon, 128 GB RAM).
 - Montaż zewnętrznej macierzy dyskowej RAID z redundantnym zasilaniem.
 - Wyposażenie serwerów w 10 dysków twardych 3,5" (pojemność 20TB każdy) oraz 2 dyski SAS 2,5" (2,4TB).
 - Dostawa i montaż centralnych systemów zasilania gwarantowanego (2 zasilacze UPS o mocy 10kVA z modułami bateryjnymi oraz 2 zasilacze UPS o mocy 3kVA).
- **Sieć LAN:** Montaż i uruchomienie 6 przełączników sieciowych (Switch Lancom GS-3126XP, 24 porty PoE) wraz z wkładkami światłowodowymi SFP+ 10Gb/s i kablami połączeniowymi DAC.
- **Stanowiska operatorskie (klienckie):**
 - Instalacja 3 stacji klienckich przystosowanych do obsługi 4 monitorów każda.
 - Montaż 9 monitorów 32" przystosowanych do pracy ciągłej (24/7).
 - Instalacja 2 pulpitów sterujących funkcjami krosowniczymi.

4. Kontrolę dostępu i systemy blokad (rok 2027)

- Montaż fizycznych barier dostępu: Instalacja 2 elektromechanicznych bramek obrotowych (kołowrotów blokujących) o wysokości do 1,5 m.
- Towarzyszące roboty budowlane: Prace budowlano-montażowe i wykończeniowe niezbędne do prawidłowego osadzenia i podłączenia bramek w budynku.

5. Prace programistyczne, integracyjne i uruchomieniowe

- Wdrożenie oprogramowania VMS: Instalacja i konfiguracja platformy Qognify VMS Infinity (licencje bazowe, kamerowe oraz pakiety wsparcia SMA na 100 kanałów IP).
- Wdrożenie systemu analityki (LPR): Konfiguracja modułu i 2 licencji do automatycznego rozpoznawania tablic rejestracyjnych.
- Integrację systemów bezpieczeństwa: Instalacja oprogramowania zarządzającego *ExSitu* (licencja serwerowa i kliencka) integrującego systemy:
 - Sygnalizacji Pożarowej (SSP – do 512 elementów),
 - Kontroli Dostępu (KD – do 512 elementów),
 - Sygnalizacji Włamania i Napadu (SSWiN – do 512 elementów),
 - Telewizji dozorowej (CCTV).
- Konfigurację zaawansowaną: Uruchomienie klastra wysokiej dostępności (High Availability), konfigurację przełączników, uruchomienie 86 linii transmisji wizji oraz pełne zaprogramowanie stanowisk operatorskich.

6. Prace formalno-organizacyjne

- Sporządzenie pełnej dokumentacji projektowej oraz uzgodnień formalnych.
- Przeprowadzenie szkoleń dla obsługi oraz wykonanie dokumentacji powykonawczej.

1.2 Ogólne uwarunkowania wykonania przedmiotu zamówienia

- **Ciągłość operacyjna urzędu:** Wszelkie prace instalacyjne i budowlane muszą być prowadzone w sposób bezwzględnie umożliwiający nieprzerwane i bezpieczne funkcjonowanie jednostek prokuratury.
- **Harmonogram prac głośnych:** Prace generujące znaczny hałas lub uciążliwość (wiercenia, kucie tras kablowych, bruzdowanie) należy realizować poza godzinami urzędowania (w godzinach popołudniowych lub w dni wolne od pracy).
- **Poufność informacji:** Ze względu na specyfikę obiektu, dokładne lokalizacje urządzeń, tras kablowych oraz szaf dystrybucyjnych mają charakter niejawny. Wykonawca uzyska do nich dostęp wyłącznie po podpisaniu Oświadczenia o zachowaniu poufności (NDA).
- **Weryfikacja personelu:** Wszyscy pracownicy Wykonawcy dedykowani do prac na terenie obiektu muszą posiadać status osób niekaranych i poddać się procedurze autoryzacji wstępu przez wewnętrzne służby ochrony Zamawiającego.

Elementy robót wskazane w pkt 1 przedmiaru robót, Wykonawca wykona najpóźniej w terminie do dnia 18 grudnia 2026 r., a pozostałą ich część (element 2) nie później niż do 31 marca 2026 r. W terminie 14 dni od zawarcia umowy Wykonawca zobowiązany jest do przedłożenia zamawiającemu Szczegółowego kosztorysu ofertowego, zgodnego z przedmiarem robót oraz złożoną ofertą.

1.3 Ogólne właściwości funkcjonalno-użytkowe

System ma na celu całodobowy nadzór wizyjny oraz kontrolę ruchu osobowego w miejscach strzeżonych wewnątrz budynku. Architektura systemu ma ułatwić służbom porządkowym szybkie reagowanie na zagrożenia oraz uprościć weryfikację materiału dowodowego. System bramek obrotowych służy jako punkt fizycznej weryfikacji uprawnień wejścia oraz moduł rejestracji czasu pracy. Cała instalacja monitoringu wizyjnego (CCTV/VSS) realizowana jest w cyfrowej technologii IP, w oparciu o architekturę klient-serwer. System bazuje na modułach zadaniowych połączonych za pomocą protokołu TCP/IP, co zapewnia dowolną skalowalność i łatwą rozbudowę. Oprogramowanie nadzoru wizyjnego uruchamia się automatycznie jako usługa systemowa bezpośrednio po starcie serwera oraz zapewnia automatyczny zapis awaryjny (przełączenie na serwer zapasowy w czasie do 2 minut) oraz zastosowanie środowiska klastra wysokiej dostępności z macierzami RAID. System integruje nowo projektowany monitoring VSS z istniejącymi na obiekcie instalacjami (SSWiN, SKD, Systemem Sygnalizacji Pożarowej (SSP / SAP).

Prezentacja wszystkich informacji będzie się odbywała w ujednolicony sposób z poziomu jednej aplikacji, przy użyciu wektorowych i wielopoziomowych map graficznych obiektu z interaktywnymi ikonami. System automatycznie mapuje zagrożenia na czytelne tabliczki alarmowe, wskazuje operatorowi lokalizację zdarzenia i uruchamia automatyczne relacje lub komunikaty pomiędzy systemami (np. automatyczne przypisanie i przywołanie obrazu z właściwej kamery po wyzwoleniu alarmu).

2. WYMAGANIA ZAMAWIAJĄCEGO ODNOSZĄCE SIĘ DO SYSTEMÓW

2.1 Centralna Platforma Zarządzająca i Integrator (VMS/SMS)

Nowo wdrażany system musi opierać się na nowoczesnej, jednolitej i otwartej architekturze klient-serwer w środowisku 64-bitowym z interfejsem w języku polskim. Oprogramowanie integrujące musi umożliwiać centralne zarządzanie z poziomu jednego interfejsu graficznego (opartego na interaktywnych, wielopoziomowych mapach wektorowych obiektu) następującymi systemami:

- Nowo projektowanym systemem monitoringu wizyjnego IP (VSS/CCTV),
- Istniejącym systemem kontroli dostępu (SKD) wraz z obsługą nowych czytników i bramek,
- Istniejącym systemem sygnalizacji włamania i napadu (SSWiN),
- Istniejącym systemem sygnalizacji pożarowej (SAP) - w celu weryfikacji wizyjnej alarmów pożarowych (automatyczne wywołanie strumienia z najbliższej kamery).

Główne wymagania funkcjonalne platformy:

- **Skalowalność i wydajność:** Licencja na startcie musi obsługiwać i archiwizować minimum 100 kanałów wideo z możliwością dalszej rozbudowy.
- **Dynamiczny multi-streaming:** Automatyczny dobór wyświetlanego strumienia w zależności od podziału okien na monitorach stacji klienckich (np. pełny ekran = strumień 4K; podział powyżej 4-9 kamer = automatyczne przełączenie na strumienie pomocnicze VGA/D1) w celu optymalizacji obciążenia sieci i procesorów.
- **Niezawodność (Failover):** System musi zapewniać funkcję automatycznego zapisu awaryjnego (High Availability). Przełączenie na serwer zapasowy z udostępnieniem obrazu musi nastąpić w czasie nie dłuższym niż 2 minuty od awarii serwera podstawowego, z późniejszą automatyczną synchronizacją danych po przywróceniu sprawności.
- **Zgodność z RODO:** Szyfrowane połączenia klienckie, wymuszenie eksportu materiału dowodowego zabezpieczonego hasłem oraz zaawansowany moduł automatycznej, dynamicznej anonimizacji (rozmywania) twarzy osób postronnych na nagraniach.

2.2 Wymogi Cyberbezpieczeństwa (KSC / NIS2 / CER)

Z uwagi na charakter jednostki publicznej wchodzącej w skład infrastruktury wrażliwej państwa, wdrażane rozwiązania technologiczne, urządzenia oraz oprogramowanie muszą bezwzględnie spełniać aktualne wymagania w zakresie bezpieczeństwa informacji, w tym pozostawać w pełnej zgodności z Ustawą o Krajowym Systemie Cyberbezpieczeństwa oraz dyrektywami NIS2 i CER. W szczególności nakłada się wymagania:

- Zakaz stosowania urządzeń od producentów, którzy w jakimkolwiek państwie członkowskim UE lub NATO zostali objęci ograniczeniami w sektorze publicznym lub krytycznym.
- Wymóg stosowania w kamerach certyfikowanych sprzętowych chipsetów szyfrujących (FIPS/TPM).

- Szyfrowanie end-to-end transmisji strumieni wideo oraz danych kontrolnych przy użyciu bezpiecznych protokołów TLS/HTTPS.
- Zapewnienie przez producenta sprzętu i oprogramowania regularnych, gwarantowanych aktualizacji firmware (łatek bezpieczeństwa) w całym okresie eksploatacji.

2.3. Struktura sieciowo-szkieletowa i punkty dystrybucyjne

Architektura logiczno-strukturalna nowej sieci dedykowanej dla systemów bezpieczeństwa musi zostać zrealizowana w oparciu o okablowanie miedziane kategorii 6A oraz magistrale światłowodowe jednomodowe (SM) minimum 4J łączące główne węzły systemu.

Węzły dystrybucyjne i lokalizacja sprzętu:

- **Główny Punkt Dystrybucyjny (GPD)** – zlokalizowany w pomieszczeniu Administratora. Wyposażony w szafę RACK 19" 42U, w której należy zainstalować: Serwery Rejestrująco-Integrujące, Centralną Macierz Dyskową w konfiguracji sprzętowej RAID, przełączniki rdzeniowe warstwy 3 (SWITCH 5 i SWITCH 6 połączone kaskadowo (Direct Attach Copper) oraz centralne systemy zasilania awaryjnego UPS.
- **Pośredni Punkt Dystrybucyjny (PPD)** – zlokalizowany w pomieszczeniu Kancelarii Niejawnej. Wyposażony w szafę RACK 19" 42U, zawierającą przełączniki obiektowe (SWITCH 1, SWITCH 2, SWITCH 3, SWITCH 4 połączone szeregowo kablami DAC) dedykowane do obsługi kamer oraz zestaw konwerterów sygnału umożliwiających wtórne wykorzystanie istniejących tras okablowania koncentrycznego.
- **Magistrala GPD - PPD** – redundantne połączenie światłowodowe jednomodowe wpięte bezpośrednio w porty uplink (1x GE SFP) pomiędzy krańcowymi przełącznikami obu szaf (SWITCH 1 - SWITCH 5 oraz SWITCH 4 - SWITCH 6).
- **Stanowiska Klientkie Ochrony** – ulokowane w pomieszczeniach ochrony nr 1 oraz nr 2. Wyposażone w zaawansowane stacje robocze obsługujące po 4 monitory profesjonalne 32" dedykowane do pracy ciągłej 24/7/365, realizujące funkcję interaktywnej ściany monitorów.
- **Zasilanie awaryjne UPS:** Podtrzymanie urządzeń w punktach dystrybucyjnych (GPD, PPD) przez min. 30 minut, natomiast dla stacji klienckich ochrony przez min. 10 minut.

3.4. Wymagania dla urządzeń i czytników dwuzakresowych (SKD / bramki)

W holu głównym budynku wymagana jest całkowita wymiana istniejących, wyeksploatowanych bramek obrotowych na nowoczesne konstrukcje modułowe o wysokiej odporności mechanicznej, zintegrowane z nowym systemem kontroli dostępu.

Kluczowe parametry techniczno-użytkowe bramek i czytników:

- **Dwuetaпова mechaniczna blokada:** Zabezpieczenie przed siłowym przepchnięciem i wandalizmem oparte na hamulcu elektromagnetycznym oraz mechanicznym zespole zapadek sterowanych cewkami na kole zębatym.

- **Wspomaganie i płynność:** Mechanizm wyposażony w elektromechaniczny układ wspomagania obrotu ramion silnikiem z paskiem zębatym, sprzęgło kulkowe dostosowujące opór do dynamiki przejścia oraz układ amortyzacji.
- **Bezpieczeństwo PPOŻ (Ewakuacja):** Obowiązkowa funkcja automatycznego, grawitacyjnego opadania ramienia bramki w przypadku zaniku zasilania elektrycznego lub po otrzymaniu sygnału alarmu pożarowego z centrali SAP.
- **Czytniki dwuzakresowe (Dual Frequency):** Fabrycznie wbudowane w obudowę bramek czytniki zbliżeniowe zdolne do jednoczesnej obsługi niskiej częstotliwości 125 kHz (standard Unique EM4102) na potrzeby obsługi dotychczasowych kart pracowników oraz wysokiej częstotliwości 13.56 MHz (standard MIFARE® DESFire® EV2/EV3) na potrzeby docelowego, w pełni bezpiecznego standardu szyfrowanego.
- **Obsługa sektorów i kluczy szyfrujących:** Dostarczone czytniki muszą umożliwiać bezproblemowy odczyt zaszyfrowanych numerów seryjnych (CSN/UID) lub dedykowanych numerów aplikacyjnych zapisanych w bezpiecznych sektorach pamięci kart (zgodnie z obecną strukturą danych i kluczami szyfrującymi używanymi przez Prokuraturę).
- **Zasada „Jednej Karty”:** Wykonawca zobowiązany jest do takiej konfiguracji urządzeń, aby pracownicy Zamawiającego mogli posługiwać się dotychczasowymi, wydanymi kartami dostępu zarówno w starych strefach SKD, jak i przy przejściu przez nowo zamontowane bramki obrotowe w holu głównym.
- **Wsparcie dla programowania:** Oprogramowanie integrujące musi posiadać pełną funkcjonalność zarządzania uprawnieniami oraz wydawania/programowania kart dostępu w tym konkretnym standardzie bezpośrednio z poziomu stacji klienckiej administratora.
- **Scenariusz Przejściowy (Migracja systemu):** Czytniki zainstalowane przy nowych bramkach obrotowych muszą w pierwszym etapie bezbłędnie identyfikować użytkowników posługujących się dotychczasowymi kartami 125 kHz Unique. W drugim etapie, po sukcesywnym wdrożeniu przez Zamawiającego nowych kart dwuzakresowych lub docelowych kart 13,56 MHz, czytniki muszą realizować bezpieczny odczyt z zaszyfrowanych sektorów pamięci nowych kart, bez konieczności modyfikacji sprzętowej czytników.

2.5. Parametry sprzętowe (matryca specyfikacji)

Poniższe tabele definiują bezwzględne minima techniczne dla kluczowych urządzeń aktywnych systemu. Zastosowanie urządzeń o parametrach gorszych skutkować będzie odrzuceniem oferty na etapie przetargu.

Tabela 1. Minimalne parametry serwerów, macierzy i stacji roboczych

Typ urządzenia	Wymagane parametry minimalne	Gwarancja
Serwer Rejestrujący (1U)	Montaż RACK, obsługa dysków Hot-swap. System operacyjny na 2x SSD min. 480GB w RAID-1. Procesor min. 10-rdzeniowy (Passmark $\geq 30\,000$ pkt), opcja instalacji 2 procesorów. Pamięć min. 128 GB RAM ECC. Interfejsy sieciowe: min. 2x 1GbE oraz min. 2x 10GbE. Zasilacz redundantny 1+1 hot-plug. Kontroler sprzętowy RAID.	5 lat
Macierz Dyskowa RACK	Podwójny redundantny kontroler, transfer min. 12 Gbit/s, pamięć RAM kontrolera min. 8GB. Zasilacz redundantny min. 2x 450W. Obsługa min. 12 dysków 2.5"/3.5". Dla VSS: konfiguracja dysków w układzie RAID-5 + 1 dysk Hot-spare. Dla integratora: 2x dyski SAS 2.4TB w RAID-1. Zapewnienie ciągłego zapisu 30 dni w pełnej jakości.	5 lat
Stacja Klientka Ochrony	Procesor min. 8-rdzeniowy (Passmark $\geq 40\,000$ pkt). Pamięć RAM min. 32 GB DDR5. Dysk podstawowy SSD min. 480GB. Dedykowana karta graficzna z obsługą 4 monitorów jednocześnie (pamięć karty min. 12GB). Interfejsy: RJ45 1GbE, DisplayPort 1.4, USB 3.0. System operacyjny 64-bit z pełną obsługą Active Directory.	5 lat

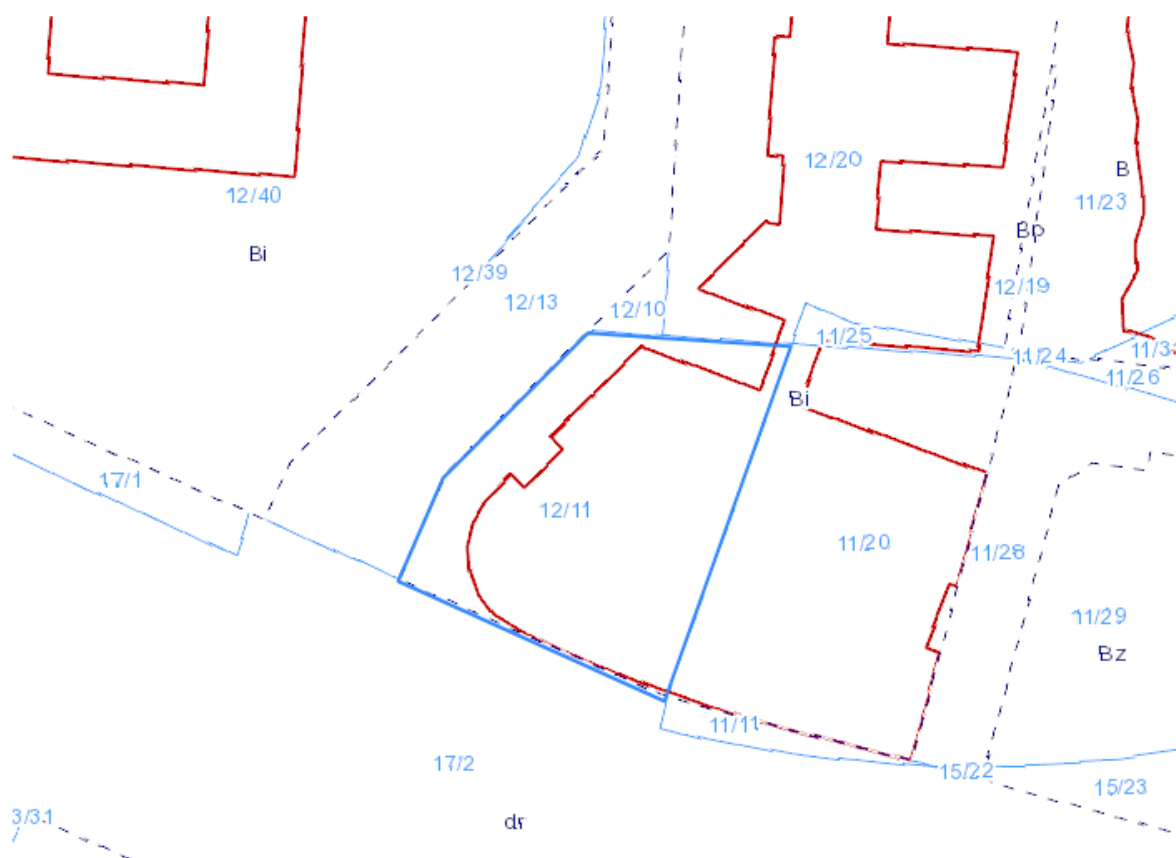
Tabela 2. Minimalne parametry kamer i przełączników sieciowych

Typ urządzenia	Wymagane parametry minimalne
Kamera Tubowa (Zewnętrzna)	Matryca 1/2.8" CMOS, rozdzielczość 8 MP (3840×2160), do 30 kl/s. Obiektyw regulowany motozoom 2.7–13.5 mm. Światłoczułość 0.005 lx, zasięg promiennika IR do 60 m. Kodowanie H.265/H.264 (3 strumienie). Funkcje: WDR 120 dB, 3D DNR. Klasa szczelności IP67, odporność IK10. Wbudowana analityka AI (zliczanie osób, detekcja intruza, loitering, SMD). Wyposażona w puszkę montażową. Gwarancja 5 lat.
Kamera Kopułowa (Wewnętrzna)	Matryca 1/2.8" CMOS, rozdzielczość 5 MP (2592×1944), do 30 kl/s. Obiektyw motozoom 2.7–13.5 mm. Zasięg promiennika IR do 50 m. Funkcje: WDR 120 dB, 2D/3D DNR. Obsługa kart SD. Interfejs audio wej/wyj (full duplex). Szczelność IP67, odporność IK10. Analityka AI analogiczna jak w kamerach tubowych. Wyposażona w puszkę montażową. Gwarancja 5 lat.
Kamera Obrotowa PTZ	Matryca 1/2.8" CMOS, rozdzielczość 5 MP (2592×1944). Obiektyw zmiennoogniskowy min. 5.5–95 mm (zoom optyczny). Zasięg IR do 150 m. Klasa szczelności IP66, odporność IK10. Zasilanie PoE+ lub AC/DC. Zaawansowana analityka: autotracking, detekcja twarzy, przecięcie linii, detekcja zmiany sceny. Gwarancja 5 lat.
Przełącznik 24 portowy PoE L3	Zarządzalny warstwy 3, 24 porty Ethernet Gigabit z obsługą PoE/PoE+ (IEEE 802.3af/at). Budżet mocy PoE min. 370 W. Porty uplink: min. 4 porty 10G SFP+. Przepustowość min. 65 Gb/s, przetwarzanie pakietów min. 50 MPPS. Bezpieczeństwo: kontrola 802.1X na portach, SSH, SSL, TACACS+, SNMPv3. Obsługa ramek Jumbo, tablica 16k MAC. Gwarancja 5 lat.

CZĘŚĆ II – informacyjna programu funkcjonalno-użytkowego

Budynek prokuratur poznańskich przy ulicy Solnej 10 w Poznaniu, w którym realizowane będzie zamierzenie budowlane usytuowany jest na terenie działek ewidencyjnych nr 12/2, 12/10, 12/11, 11/20 oznaczonych w ewidencji gruntów i budynków symbole BI. Budynek położony jest na terenie objętym Planem ogólnym Miasta Poznania uchwalonym Uchwałą Br XXIX/529/IX/2025 z dnia 30 grudnia 2025 r. oznaczonym symbolem 527SU – Strefa usługowa.

Informacja o zagospodarowaniu terenu



Zamawiający oświadcza, że ma prawo do dysponowania nieruchomościami, w których przewidziano realizację robót budowlanych i dostarczy Wykonawcy stosowne dokumenty w trakcie realizacji przedmiotu zamówienia.

Przepisy prawne i normy związane z projektowaniem i wykonaniem przedmiotu zamówienia:

1. Ustawa z dnia 29 stycznia 2004r. Prawo zamówień publicznych (Dz. U.2026r.793 ze zm.).
2. Ustawa z dnia 7 lipca 1994r. Prawo Budowlane (Dz. U. z 2026.524 ze zm.).
3. Ustawa z dnia 27 kwietnia 2001r. o odpadach (Dz. U. 2023.1587 ze zm.).
4. Ustawa z dnia 16 kwietnia 2004r. o wyrobach budowlanych (Dz. U. 2021.1213).
5. Ustawa z dnia 24 sierpnia 1991r. o ochronie przeciwpożarowej (Dz. U. 2025.188).
6. Rozporządzenie Ministra Infrastruktury z dnia 26 października 2005r. w sprawie warunków technicznych jakim powinny odpowiadać telekomunikacyjne obiekty budowlane i ich usytuowanie (Dz. U. z 2005r. Nr 219, poz. 1864).
7. Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002r. w sprawie warunków technicznych jakim powinny odpowiadać budynki i ich usytuowanie (Dz. U. 2022.1225 ze zm.).
8. Rozporządzenie Ministra Infrastruktury z dnia 3 lipca 2003r. w sprawie szczegółowego zakresu i formy projektu budowlanego (Dz. U. 2022.1679 ze zm.).
9. Rozporządzenie Ministra Infrastruktury z dnia 2 września 2004r. w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego (Dz. U. 2021.2454 ze zm.).
10. Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 5 sierpnia 2023r. w sprawie uzgadniania projektu zagospodarowania działki lub terenu, projektu architektoniczno-budowlanego, projektu technicznego oraz projektu urządzenia przeciwpożarowego pod względem zgodności z wymaganiami ochrony przeciwpożarowej (Dz. U. 2023.1563 ze zm.).
11. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 kwietnia 2006r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz. U. 2023.822 ze zm.).
12. Rozporządzenie Ministra Infrastruktury z dnia 23 czerwca 2003r. w sprawie informacji dotyczącej bezpieczeństwa i ochrony zdrowia oraz planu bezpieczeństwa i ochrony zdrowia (Dz. U. z 2003r. Nr 120, poz. 1126).

Wykonawca zrealizuje zamówienie zgodnie z najnowszymi wydaniem norm:

- **PN-EN 62676** (części 1-1, 1-2, 2-1, 4) – Systemy dozorowe VSS/CCTV.
- **PN-EN 50173-1, 50174-1, 50174-2, 50174-3, 50310** – Projektowanie i budowa sieci informatycznych i okablowania strukturalnego.

Dokumenty i informacje niezbędne do zaprojektowania robót budowlanych, w tym posiadana przez Zamawiającego dokumentacja powykonawcza obejmująca inwentaryzację systemów podlegających przebudowie zostanie udostępniona Wykonawcy po podpisaniu oświadczenia o zachowaniu poufności (NDA). Dodatkowe wytyczne inwestorskie i uwarunkowania związane z planowaną inwestycją określa dokument pn. „Dokumentacja techniczna Modernizacja systemu monitoringu wizyjnego oraz kontroli dostępu w budynku Prokuratury Poznańskich przy ulicy Solnej 10 w Poznaniu opracowana w lipcu 2026 r. przez Przedsiębiorstwo Handlowo-Usługowe NET KOM Tomasz Klemeński.

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy wykażą, że w okresie ostatnich 5 lat należycie wykonali **co najmniej 2 (dwa) zadania**, z których każde polegało na zaprojektowaniu i wykonaniu (lub wykonaniu) systemów bezpieczeństwa w budynku

użyteczności publicznej lub obiekcie infrastruktury krytycznej o wartości minimum **500 000,00 PLN brutto** każde. W ramach każdego z wykazanych zadań Wykonawca musi udowodnić wdrożenie i pełną integrację oprogramowania dla min. 80 kamer IP, 20 przejść SKD (w tym bramki obrotowej) oraz systemów alarmowych (SSWiN lub SAP).

Zgodnie z art. 121 ustawy Prawo zamówień publicznych, Zamawiający zastrzega obowiązek osobistego wykonania przez Generalnego Wykonawcę następujących kluczowych prac: projektowanie algorytmów integracji i scenariuszy makro platformy VMS, konfiguracja oprogramowania integrującego i budowa map wektorowych oraz implementacja modułów cyberbezpieczeństwa i RODO. Powierzenie tych prac podwykonawcom skutkować będzie naliczeniem kary umownej w wysokości **20 000,00 PLN** za każdy przypadek naruszenia.

Ocena ofert zostanie dokonana w oparciu o trzy kryteria zintegrowane w Formularzu Ofertowym:

- **Kryterium 1: Cena całkowita brutto** – Waga: 60% (maks. 60 pkt). Przyznawane na zasadzie proporcji najniższej ceny do ceny badanej.
- **Kryterium 2: Wydłużony okres gwarancji** – Waga: 20% (maks. 20 pkt). Próg minimalny (wymagany) to 60 miesięcy (0 pkt). Wydłużenie do 72 miesięcy = 10 pkt; wydłużenie do 84 miesięcy i więcej = 20 pkt.
- **Kryterium 3: Czas reakcji serwisu na awarię krytyczną** – Waga: 20% (maks. 20 pkt). Deklaracja czasu reakcji w reżimie 24/7/365: powyżej 4h do 8h = 0 pkt; do 4h = 5 pkt; do 2h = 10 pkt; do 1h = 20 pkt.

W okresie trwania gwarancji jakości Wykonawca zobowiązany jest do bezpłatnego, całodobowego utrzymania systemów w pełnej sprawności operacyjnej. Zdarzenia serwisowe klasyfikowane są jako:

- **Awaria Krytyczna (AK):** Zdarzenie uniemożliwiające rejestrację lub podgląd z min. 10% kamer IP, awaria serwera głównego lub macierzy, brak komunikacji platformy integrującej z systemami SAP/SKD/SSWiN, całkowita blokada bramki obrotowej w holu głównym lub awaria centralnego UPS.
- **Awaria Zwykła (AZ):** Dysfunkcja pojedynczych elementów (np. uszkodzenie jednej kamery wewnętrznej, pojedynczego czytnika przy drzwiach bocznych), która nie paraliżuje globalnego bezpieczeństwa obiektu.

Ustala się matrycę reżimów czasowych i kar umownych:

Klasa zdarzenia	Czas reakcji serwisu	Czas na pełną naprawę	Kara umowna za zwłokę
Awaria Krytyczna (AK)	Zgodnie z ofertą (max 1h - 8h)	Maksymalnie 12 godzin (lub podstawienie sprzętu zastępczego)	500 PLN za każdą godzinę zwłoki w reakcji; 2000 PLN za każdy dzień zwłoki w naprawie

Awaria Zwykła (AZ)	Maksymalnie 12 godzin	Maksymalnie 48 godzin	500 PLN za każdy dzień zwłoki w naprawie
--------------------	-----------------------	-----------------------	--

W przypadku, gdy Wykonawca nie podejmie działań zmierzających do usunięcia zgłoszonej Awarii Krytycznej w czasie dłuższym niż 24 godziny od momentu zgłoszenia, Zamawiający zastrzega sobie prawo do powierzenia usunięcia awarii podmiotowi trzeciemu na koszt i ryzyko Wykonawcy (**wykonanie zastępcze**), bez utraty praw do gwarancji głównej udzielonej przez Wykonawcę na cały system.