

Wnioskodawca:

Michał Kirszling – Kierownik Działu Infrastruktury Sportowej

OPIS PRZEDMIOTU ZAMÓWIENIA

(zamówienia wieloasortymentowe dla dostaw – w zależności od specyfiki zamówienia można zastosować własny formularz)

I. Nazwa zadania: Dostawa, montaż i konfiguracja elementów systemu IT (serwer, oprogramowanie do monitoringu, oprogramowanie do zarządzania i monitorowania IT)

1. Przedmiot zamówienia część 2:

Dostawa i konfiguracja oprogramowania do monitoringu wraz z dodatkową licencją na 50 kamer oraz wymianą dysków w serwerze.

2. Wymagania ogólne:

1. Zakres prac:

Zamówienie obejmuje dostawę i fizyczny montaż nowych dysków twardych w istniejącym serwerze Zamawiającego wraz z rekonfiguracją macierzy dyskowej (RAID). Przedmiotem zamówienia jest również dostawa, instalacja i pełna konfiguracja fabrycznie nowego oprogramowania do zarządzania systemem monitoringu wizyjnego. Wykonawca dostarczy i zintegruje z oprogramowaniem bazowym 150 licencji kanałowych, pozwalających na obsługę kamer IP. Prace obejmują uruchomienie całości środowiska, dodanie istniejących kamer do systemu oraz przeprowadzenie testów akceptacyjnych.

2. Stan prawny i techniczny sprzętu (Dyski twarde):

Wszystkie oferowane dyski twarde muszą być fabrycznie nowe, pochodzić z oficjalnego i autoryzowanego kanału sprzedaży producenta na rynek europejski. Oferowany sprzęt musi być wolny od wad fizycznych i prawnych. Bezwzględnie wyklucza się dostawę sprzętu używanego, odnawianego (refurbished) lub pochodzącego z demontażu. Dyski muszą być przeznaczone do pracy ciągłej 24/7 w zaawansowanych systemach monitoringu lub rozwiązaniach serwerowych (klasa Enterprise) i wykorzystywać konwencjonalną technologię zapisu magnetycznego (CMR).

3. Wymagania dotyczące oprogramowania i licencji

Zaoferowane oprogramowanie do zarządzania wideo musi być aktualną wersją stabilną, w pełni wspieraną przez producenta (wyklucza się oprogramowanie w fazie End-of-Life).

Wymagane jest dostarczenie licencji bazowej (jeśli jest wymagana przez producenta) oraz **dodanie 50 licencji** na kanały wideo w modelu bezterminowym (dożywotnim).

W cenie zamówienia Wykonawca musi zapewnić plan darmowych aktualizacji oprogramowania (Software Upgrade Plan/Maintenance) na okres minimum 36 miesięcy od dnia podpisania protokołu odbioru.

4. Wymagania wdrożeniowe i organizacyjne:

Wykonawca zobowiązany jest przeprowadzić prace instalacyjne w sposób minimalizujący przestoje w pracy systemu monitoringu. Wszelkie przerwy w nagrywaniu muszą być wcześniej uzgodnione z Zamawiającym. Po fizycznej wymianie dysków Wykonawca zainstaluje odpowiedni system

operacyjny (jeśli dotyczy) oraz wdroży oprogramowanie, optymalizując je pod kątem wydajności posiadanego przez Zamawiającego serwera (Dell PowerEdge R440). Konfiguracja systemu po stronie Wykonawcy obejmuje m.in. ustawienie harmonogramów nagrywania, zdefiniowanie uprawnień dla użytkowników oraz konfigurację widoków (stacji operatorskich) zgodnie z wytycznymi Zamawiającego.

5. Gwarancja, wsparcie techniczne i szkolenia:

Na dostarczone dyski twarde Wykonawca udzieli gwarancji na okres nie krótszy niż 36 miesięcy. Czas reakcji serwisu na zgłoszenie awarii sprzętowej nie może być dłuższy niż następny dzień roboczy (NBD). Wykonawca, po bezusterkowym uruchomieniu systemu, przeprowadzi w siedzibie Zamawiającego szkolenie dla administratorów (z zakresu zarządzania systemem) oraz dla operatorów (z zakresu codziennej obsługi i eksportu nagrań). Zakończenie wdrożenia musi zostać udokumentowane przekazaniem pełnej dokumentacji powykonawczej oraz instrukcji obsługi w języku polskim.

3. Wymagania (parametry) szczegółowe w wersji tabelarycznej:

Lp.	Asortyment	J.m.	Ilość	Opis wymagań minimalnych	Uzasadnienie wymagań
1	2	3	4	5	6
1	Oprogramowanie do monitoringu	szt.	1	Minimum 320 kamer maksymalnie obsługujących przez serwer	Taka pojemność gwarantuje odpowiednią skalowalność systemu dla dużych obiektów, pozwalając na centralne zarządzanie rozbudowaną infrastrukturą bez konieczności natychmiastowego zakupu kolejnych serwerów. Zapewnia to stabilną obsługę i rejestrację obrazu z wielu punktów jednocześnie.
				Maksymalna liczba podstacji na system – Minimum 700	Zapewnia to możliwość scentralizowanego zarządzania bardzo rozległą, rozproszoną infrastrukturą z jednego miejsca. Taka skalowalność pozwala na płynny rozwój organizacji bez konieczności dzielenia systemu na mniejsze, niezależne środowiska.
				Możliwość wirtualizacji serwera na Vmware bądź Hyper-V	Wdrożenie systemu w środowisku wirtualnym pozwala na optymalne wykorzystanie posiadanych zasobów sprzętowych Zamawiającego oraz ułatwia zarządzanie kopiami zapasowymi i dostępnością. Zapewnia to elastyczność i skalowalność rozwiązania bez konieczności zakupu dedykowanego serwera fizycznego.
				Maksymalna rozdzielczość kamer obsługiwana przez system – minimum 12 megapikseli	Obsługa kamer o wysokiej rozdzielczości gwarantuje szczegółowość obrazu niezbędną do precyzyjnej identyfikacji osób i numerów rejestracyjnych na rozległych obszarach. Zapewnia to elastyczność infrastruktury i gotowość na przyszłą modernizację punktów wizyjnych.
				Możliwość obsługi audio dwukierunkowo	Funkcjonalność ta pozwala na bezpośrednią komunikację głosową operatora z osobami znajdującymi się w monitorowanym obszarze. Zwiększa to poziom bezpieczeństwa poprzez możliwość natychmiastowego reagowania na incydenty i wydawania ostrzeżeń.

			Współpraca z istniejącym systemem monitoringu – kamery Vivotek	Konieczność integracji wynika z posiadania przez Zamawiającego sprawnych urządzeń tej marki, co pozwala na ochronę dotychczasowych inwestycji sprzętowych. Zapewnia to płynne włączenie istniejących kamer do nowego, scentralizowanego środowiska bez ponoszenia dodatkowych kosztów.
			Maksymalna liczba kanałów nagrywania na grupę – minimum 320	Wymóg ten umożliwia logiczne grupowanie dużej liczby strumieni wideo, co ułatwia administrację i optymalizuje obciążenie zasobów sprzętowych. Gwarantuje to wysoką wydajność systemu przy jednoczesnym ciągłym zapisie obrazu z setek kamer.
			Nagrywanie zdarzeń	Funkcjonalność ta pozwala na automatyczne rejestrowanie obrazu tylko w momencie wystąpienia określonego incydentu (np. detekcja ruchu, przekroczenie linii, alarm). Oszczęda to przestrzeń dyskową i znacząco przyspiesza późniejsze wyszukiwanie kluczowych dowodów w archiwum wideo.
			Tryb wyświetlania „Rybie oko” - 10, 1P, 1R, 103R, 4R, 2P, 4R Pro, 108R	Różnorodne tryby wyświetlania pozwalają na sprzętowe lub programowe prostowanie szerokokątnego obrazu z kamer 360 stopni do formatów czytelnych dla operatora. Oznacza to możliwość płynnej nawigacji i analizy obrazu bez zniekształceń, co jest kluczowe przy monitorowaniu dużych powierzchni.
			Korekcja zniekształceń w trybie „Rybiego oka” - Tak	Korekcja zniekształceń (dewarping) jest niezbędna do przekształcenia surowego, sferycznego obrazu w naturalne i czytelne dla ludzkiego oka rzuty płaskie. Pozwala to operatorowi na właściwą ocenę sytuacji, odległości oraz precyzyjną identyfikację obiektów bez irytujących zakrzywień perspektywy.
			Dodatkowy czas nagrywania do rejestracji zdarzeń - Czas nagrywania przed zdarzeniem: minimum 3–15 (s); czas nagrywania po zdarzeniu: minimum 10–60 (s)	Funkcja buforowania obrazu (pre-alarm i post-alarm) gwarantuje zapisanie pełnego kontekstu incydentu, włączając w to sytuację bezpośrednio poprzedzającą zdarzenie oraz jego skutki. Zapobiega to utracie kluczowych dowodów wynikającej z ewentualnych opóźnień w detekcji sprzętowej.
			Format pliku nagrywania – między innymi 3GP	Obsługa formatu 3GP pozwala na łatwy eksport nagrań wideo w silnie skompresowanej formie, idealnej do szybkiego przesyłania materiału dowodowego drogą elektroniczną (np. na telefony komórkowe). Zapewnia to dużą elastyczność w udostępnianiu kluczowych fragmentów incydentów bez obciążania łączy sieciowych.
			Możliwość szyfrowania nagrań – minimum AES-256 CTR	Zastosowanie silnego algorytmu szyfrującego chroni wrażliwy materiał wideo przed nieautoryzowanym dostępem lub wyciekiem w przypadku kradzieży fizycznych nośników danych. Gwarantuje to pełną zgodność z rygorystycznymi

					wymogami ochrony danych osobowych (RODO) i wewnętrzną polityką bezpieczeństwa.
				Tryby odtwarzania: Asynchroniczny, synchroniczny	Odtwarzanie synchroniczne umożliwia precyzyjne śledzenie incydentu na wielu kamerach w tym samym czasie, co jest kluczowe dla pełnej analizy zdarzeń. Z kolei tryb asynchroniczny pozwala operatorowi niezależnie przeglądać różne fragmenty nagrań, optymalizując czas weryfikacji alarmów.
				Sterowanie odtwarzaniem: Sterowanie prędkością od 1/64X do 64X, następna/poprzednia klatka, wstrzymywanie, odtwarzanie, przewijanie, zatrzymywanie	Precyzyjne sterowanie prędkością oraz nawigacja poklatkowa są kluczowe do dokładnej analizy dynamicznych zdarzeń i identyfikacji drobnych szczegółów. Umożliwia to operatorom błyskawiczne przeszukiwanie długich nagrań oraz perfekcyjne zatrzymanie obrazu w najważniejszym momencie incydentu.
				Możliwość wyświetlania znaku wodnego	Znak wodny zabezpiecza wyeksportowane nagrania przed nieautoryzowaną modyfikacją i bezspornie potwierdza ich autentyczność jako materiału dowodowego. Dodatkowo chroni to prawa własności Zamawiającego w przypadku udostępniania plików wideo organom ścigania lub podmiotom trzecim.
				Inteligentne wyszukiwanie ludzi i pojazdów	Zaawansowana analityka wideo znacznie skraca czas przeszukiwania archiwum, pozwalając na błyskawiczne odnalezienie nagrań z udziałem konkretnych typów obiektów. Funkcjonalność ta automatyzuje pracę operatorów, eliminując konieczność wielogodzinnego, ręcznego przeglądania materiału dowodowego.
				Inteligentne wyszukiwanie cech: ludzie: płeć, wiek, kolor ubrania, akcesoria; pojazdy: rodzaj, kolor	Szczegółowe filtrowanie nagrań po atrybutach obiektów drastycznie przyspiesza dochodzenia, umożliwiając błyskawiczne zlokalizowanie osoby lub pojazdu na podstawie szczegółowego rysopisu. Znacząco podnosi to efektywność pracy operatorów, zdejmując z nich konieczność ręcznego przeglądania setek godzin materiału.
				Inteligentne wyszukiwanie zachowań : przekroczenie linii, wtargnięcie, wałęsanie się	Automatyczna detekcja specyficznych zachowań pozwala na natychmiastowe wykrywanie naruszeń stref zastrzeżonych oraz identyfikację podejrzaną aktywności. Znacząco przyspiesza to weryfikację incydentów w archiwum bez konieczności ciągłego, ręcznego monitorowania obrazu przez operatora.
				Inteligentne ponowne wyszukiwanie po podobnym wyglądzie	Funkcja ta umożliwia błyskawiczne śledzenie trasy przemieszczania się wybranej osoby lub pojazdu na przestrzeni całego obiektu, bazując wyłącznie na ich wyglądzie. Znacząco podnosi to efektywność pracy dochodzeniowej, eliminując potrzebę ręcznego analizowania nagrań z kolejnych kamer w poszukiwaniu tego samego obiektu.

			Informacja o zdarzeniach na rejestratorach i stacjach: Błąd pamięci, brak wolnej pamięci, brak połączenia z siecią	Bieżące monitorowanie stanu technicznego urządzeń rejestrujących pozwala na natychmiastową reakcję na awarie sprzętowe lub problemy sieciowe. Zapobiega to utracie ciągłości nagrań i gwarantuje stabilne funkcjonowanie całego systemu bezpieczeństwa.
			Informowanie o statusie alarmu	Jasna informacja o aktualnym stanie alarmu (np. nowy, w weryfikacji, zamknięty) pozwala na sprawne zarządzanie incydentami przez wielu operatorów jednocześnie. Zapobiega to pominięciu krytycznych zdarzeń lub niepotrzebnemu dublowaniu pracy nad tą samą sprawą.
			Sterowanie PTZ(sterowanie w pionie i poziomie): przeciąganie i przenoszenie myszką, kliknięcie w celu przeniesienia, manipulator	Różnorodne metody sterowania kamerami obrotowymi zapewniają operatorowi maksymalną ergonomię i szybkość reakcji podczas śledzenia poruszających się obiektów. Zwiększa to precyzję nadzoru wizyjnego i pozwala na natychmiastowe dostosowanie pola widzenia do dynamicznie zmieniającej się sytuacji.
			Sterowanie PTZ(zbliżenia)Przeciąganie i przenoszenie myszką, kliknięcie w celu przeniesienia, manipulator	Intuicyjne sterowanie przybliżeniem obrazu pozwala na błyskawiczną weryfikację detali, takich jak twarze czy tablice rejestracyjne, co jest kluczowe podczas śledzenia obiektów. Zapewnia to operatorowi pełną i precyzyjną kontrolę nad obiektywem z wykorzystaniem preferowanego urządzenia wskazującego.
			Możliwość tworzenia E-map:	Zastosowanie interaktywnych planów obiektu (E-map) zapewnia operatorom szybką orientację przestrzenną i pozwala na natychmiastowe zlokalizowanie źródła alarmu. Jest to niezbędne do sprawnego i intuicyjnego zarządzania systemem bezpieczeństwa, szczególnie w rozległych budynkach lub na dużych terenach zewnętrznych.
			Możliwość rozpoznawania tablic rejestracyjnych	Funkcjonalność ta (LPR/ANPR) jest niezbędna do automatyzacji kontroli dostępu pojazdów na teren obiektu oraz błyskawicznego identyfikowania poszukiwanych aut. Eliminuje to błędy ludzkie przy ręcznym weryfikowaniu numerów i drastycznie skraca czas przeszukiwania materiału dowodowego.
			Możliwość tworzenia ścian video Matrix	Funkcjonalność zarządzania ścianą wideo (Video Wall) jest niezbędna w głównym centrum nadzoru do jednoczesnego monitorowania dużej liczby kamer. Zapewnia to operatorom maksymalną świadomość sytuacyjną i pozwala na sprawne, zespołowe koordynowanie działań poprzez wyświetlanie kluczowych obrazów na wielkoformatowych zestawach monitorów.
			Praca w trybie awaryjnym CMS: Redundancja 1+1	Architektura ta zapewnia najwyższy poziom niezawodności i ciągłość działania systemu zarządzania monitoringiem (CMS). W przypadku awarii sprzętowej lub sieciowej

					serwera głównego, jego zadania automatycznie przejmują serwery zapasowe, eliminując przestoje i ryzyko utraty kontroli nad całym systemem.
				Praca w trybie podstacja: Redundancja NxM	Architektura ta gwarantuje ciągłość zapisu obrazu w rozbudowanych systemach wieloserwerowych, optymalizując jednocześnie koszty sprzętowe. W przypadku awarii jednego lub kilku z „N” serwerów nagrywających (produkcyjnych), ich zadania automatycznie przejmują wyznaczone z puli „M” serwery zapasowe, co zapobiega bezpowrotnej utracie krytycznego materiału dowodowego.
	Dysk twardy do monitoringu	szt.	4	Pojemność: min 16 TB	Znacząca rozbudowa systemu (dodanie 50 nowych punktów kamerowych) oraz konieczność zachowania długiego okresu retencji (przechowywania) nagrań w wysokiej rozdzielczości wymuszają drastyczne zwiększenie przestrzeni magazynowej. Ze względu na fizyczne ograniczenia posiadanego serwera (limitowana liczba zatok dyskowych), zastosowanie dysków o minimalnej pojemności 16 TB jest krytyczne do zbudowania macierzy gwarantującej ciągłość zapisu, bez ryzyka przedwczesnego nadpisania ważnego materiału dowodowego.
				Interfejs: SAS 12 Gb/s	Interfejs SAS (Serial Attached SCSI) o przepustowości 12 Gb/s oferuje komunikację w pełnym duplexie (jednoczesny odczyt i zapis danych), co jest technologicznie nieosiągalne dla tańszych dysków SATA. W środowisku monitoringu wizyjnego, gdzie serwer musi nieprzerwanie zapisywać potężne strumienie wideo z 200 kamer i jednocześnie umożliwiać operatorom szybkie przeszukiwanie archiwum, interfejs SAS zapobiega powstawaniu tzw. wąskich gardeł (bottlenecks) i gwarantuje błyskawiczną reakcję macierzy.
				Prędkość obrotowa: min 7200 RPM	Prędkość obrotowa talerzy na poziomie 7200 obr./min gwarantuje krótki czas dostępu do danych (niskie opóźnienia) oraz wysoką przepustowość ciągłą zapisu. W systemach VMS, które muszą jednocześnie i bezprzerwy zapisywać potężne strumienie wideo z dziesiątek kamer oraz obsługiwać zapytania operatorów odtwarzających archiwum, wysoka wydajność mechaniczna jest krytyczna, aby zapobiec zjawisku gubienia klatek obrazu (frame drop).
				Pamięć podręczna (cache): min 256 MB	Odpowiednio duży i szybki bufor pamięci podręcznej dysku jest niezbędny do zarządzania ogromną liczbą jednoczesnych operacji I/O (wejścia/wyjścia). W zaawansowanych systemach monitoringu, gdzie dziesiątki kamer wysokiej rozdzielczości nieustannie

					przesyłają zmienne strumienie wideo, wbudowany cache "absorbują" nagłe piki obciążeniowe, zanim dane zostaną trwale zapisane na talerzach magnetycznych. Zapobiega to przepełnieniu buforów kontrolera RAID i bezpowrotnej utracie klatek obrazu.
				Technologia zapisu: Advanced Format 512e	Dyski w standardzie 512e (emulacja sektora 512-bajtowego przy fizycznym rozmiarze sektora 4K) są niezbędne do zagwarantowania bezproblemowej, natywnej współpracy z posiadanym przez Zamawiającego sprzętowym kontrolerem macierzowym (PERC H730P) oraz środowiskiem wirtualizacyjnym. Zastosowanie formatu 512e zapewnia optymalną wydajność i kompatybilność, eliminując ryzyko groźnych błędów przesunięcia sektorów (misalignment), niestabilności sprzętowego RAID-u oraz nagłych spadków szybkości odczytu/zapisu podczas intensywnego zrzucania nagrań.
				Typ: Hot-swap	Funkcja Hot-swap jest krytyczna dla zachowania ciągłości pracy serwera monitoringu, umożliwiając wymianę uszkodzonego nośnika bez konieczności wyłączania urządzenia i przerywania nagrywania z 200 kamer. Jest to bezpośrednio powiązane z wymogiem zachowania wysokiej dostępności usług oraz procedurami awaryjnymi, które zakładają minimalizację czasu przestoju systemu do zera w przypadku rutynowych usterek sprzętowych.
				Wymiary: standardowe dla dysków 3,5 cala	Serwer Dell PowerEdge R440 w posiadanej przez Zamawiającego konfiguracji wyposażony jest w zatoki dyskowe przystosowane do nośników 3,5 cala. Zastosowanie dysków o tym standardzie zapewnia optymalne chłodzenie oraz stabilność mechaniczną wewnątrz obudowy. Jest to również niezbędne dla zachowania pełnej ewidencji zasobów dyskowych, co jest wymagane przez wewnętrzne standardy bezpieczeństwa.
				Chłodzenie: aktywny wentylator	Zastosowanie dysków klasy Enterprise SAS 12 Gb/s o prędkości 7200 RPM generuje znaczące ilości energii cieplnej, szczególnie przy jednoczesnym zapisie z 200 kamer. Zgodnie z wytycznymi, serwerownie muszą posiadać całoroczną klimatyzację, a temperatura musi być stale monitorowana. Aktywne wymuszanie przepływu powietrza przez wentylatory serwerowe jest niezbędne, aby zapobiec awariom wynikającym z przegrzania nośników, co mogłoby naruszyć ciągłość działania systemów krytycznych.
				Kompatybilność: serwery i macierze obsługujące interfejs SAS 12 Gb/s	Posiadana przez Ośrodek infrastruktura krytyczna opiera się na rozwiązaniach serwerowych Dell oraz

					macierzowych Alcatel, które wymagają bezwzględnej, sprzętowej kompatybilności w celu zachowania ciągłości działania systemów. Zastosowanie nośników w pełni certyfikowanych do pracy z kontrolerami SAS 12 Gb/s jest niezbędne do zapewnienia redundancji i stabilności klastrów, co pozwala na skuteczne zarządzanie ryzykiem w obszarze informatyki. Brak pełnej kompatybilności (np. błędy w komunikacji firmware dysku z kontrolerem) może prowadzić do niekontrolowanych awarii macierzy i bezpowrotnej utraty danych.
	Gwarancja	miesiące	min. 36 miesięcy	Min. 36 miesięcy na dyski twarde	Zgodnie z nadrzędnym celem definiowania standardów bezpieczeństwa środowiska informatycznego, system monitoringu musi pracować w trybie ciągłym. Wykorzystanie podzespołów o najwyższym współczynniku niezawodności jest niezbędne do zarządzania ryzykiem oraz minimalizacji wystąpienia zdarzeń opisanych w rejestrze zagrożeń. Długoletnie wsparcie producenta gwarantuje, że w systemie pracować będą wyłącznie urządzenia posiadające aktualne wsparcie techniczne, co jest wymogiem bezpieczeństwa danych osobowych.

4. Szczegółowy zakres prac wdrożeniowych i wymagania techniczne dla systemu monitoringu wizyjnego (VMS):

Niniejszy dokument definiuje rygorystyczne wytyczne dotyczące modernizacji, rekonfiguracji oraz wdrożenia rozszerzonego środowiska monitoringu wizyjnego. Wdrożenie musi zostać przeprowadzone z bezwzględnym poszanowaniem polityki bezpieczeństwa środowiska informatycznego obowiązującej u Zamawiającego. Wszelkie odchylenia od poniższych standardów będą skutkować natychmiastowym przerwaniem prac oraz rozwiązaniem umowy.

Faza 1: Warstwa fizyczna i rekonfiguracja punktów kamerowych

Prace w obrębie urządzeń końcowych wymagają najwyższej staranności oraz gotowości do prac terenowych, nierzadko w trudnych warunkach i na dużych wysokościach.

- Zarządzanie pulą urządzeń: Pełna rekonfiguracja logiki działania dla maksymalnie 150 istniejących kamer IP oraz autoryzacja i dodanie licencji dla 50 nowych punktów kamerowych.
- Fizyczny dostęp i twardy reset (Wymóg bezwzględny): Wykonawca musi być przygotowany sprzętowo na fizyczne dotarcie do każdego ze 150 punktów kamerowych. W przypadku utraty danych uwierzytelniających, braku spójności oprogramowania układowego (firmware) lub niemożności nawiązania sesji zdalnej, Wykonawca jest zobligowany do fizycznego demontażu urządzenia, wykonania twardego resetu na obiekcie, ponownej kalibracji optyki oraz uszczelnienia obudowy.
- Segmentacja urządzeń: Wszystkie kamery, jako urządzenia tzw. „Internetu rzeczy”, muszą zostać bezwzględnie odseparowane i umieszczone w dedykowanej wirtualnej sieci lokalnej

(VLAN). Niedopuszczalne jest współdzielenie przestrzeni adresowej z siecią biurową lub serwerową.

Faza 2: Środowisko serwerowe, wirtualizacja i macierze dyskowe

Sercem systemu będzie klaster wirtualizacyjny. Wykonawca ponosi pełną odpowiedzialność za optymalizację warstwy hiperwizora oraz systemów operacyjnych.

- Wirtualizacja (VMware) i OS (Linux): Instalacja, utwardzenie (hardening) oraz konfiguracja maszyn wirtualnych w środowisku VMware. Systemem gościa dla usług VMS będzie rygorystycznie skonfigurowana dystrybucja systemu Linux.
- Synchronizacja czasu: Wszystkie serwery, maszyny wirtualne oraz same kamery muszą być bezwzględnie zsynchronizowane z wyznaczonym, centralnym serwerem czasu NTP.
- Macierz Alcatel i redundancja danych: Inżynieria przestrzeni dyskowej LUN na macierzy Alcatel. Wolumeny muszą być zoptymalizowane pod kątem wielowątkowego zapisu ciągłego (CCTV workload).
- Polityka Backupów: Konfiguracja mechanizmów kopii zapasowych. Wymagane jest utrzymywanie co najmniej 3 pełnych kopii zapasowych. Ponadto, z uwagi na ochronę przed atakami typu ransomware, środowisko musi gwarantować dostępność kopii typu offline. Surowo zabrania się wykonywania i wyprowadzania jakichkolwiek kopii do zewnętrznych usług chmurowych. W przypadku środowiska wirtualnego, Wykonawca zagwarantuje możliwość odtworzenia maszyn do 2 tygodni wstecz.

Faza 3: Topologia sieciowa, rekonfiguracja przełączników Cisco i UTM Fortigate

Bezpieczeństwo na krawędzi sieci oraz w warstwie dostępowej jest priorytetem najwyższego rzędu. Każde urządzenie pracujące w sieci musi podlegać autoryzacji.

- Utwardzenie infrastruktury dostępowej (Cisco): Rekonfiguracja przełączników rdzeniowych i dostępowych. Wymagane jest wdrożenie mechanizmów blokady dostępu na portach dla urządzeń nieuwierzytelnionych (np. 802.1X, system NAC lub ścisła filtracja po adresach MAC).
- Konfiguracja bramy bezpieczeństwa UTM (Fortigate):
 - * Wydzielenie precyzyjnych stref bezpieczeństwa (w tym DMZ dla usług wystawionych na zewnątrz).
 - Wdrożenie głębokiej inspekcji pakietów. Cały ruch przechodzący przez bramę (w tym szyfrowany) musi być kontrolowany pod kątem infekcji i ataków.
 - Ścisła kontrola aplikacji na firewallu: bezwzględna blokada usług typu peer-to-peer (p2p), programów zdalnego dostępu, botnetów oraz anonimowych bramek proxy.
 - Usługi zewnętrzne wystawione na UTM muszą być obligatoryjnie chronione polisami DoS (Denial of Service).

Faza 4: Autoryzacja i Zarządzanie Użytkownikami

Dostęp do potężnego narzędzia, jakim jest system monitoringu, będzie ściśle licencjonowany i kontrolowany.

- Zarządzanie dostępem: Stworzenie ról systemowych i konfiguracja dostępu dla maksymalnie 5 operatorów/administratorów.

- Integracja z Active Directory: Jeśli stacje klienckie będą pracować w domenie, uwierzytelnianie musi opierać się o istniejącą w architekturze usług katalogową (AD) firmy Microsoft.
- Polityka haseł: Hasła dla ról administracyjnych muszą spełniać kryteria najwyższej złożoności – minimum 12 znaków (małe i duże litery, cyfry, znaki specjalne). Główne poświadczenia ratunkowe muszą zostać zdeponowane przez Wykonawcę w tzw. bezpiecznych kopertach, w protokołowanym trybie przekazania.
- Dostęp zdalny: Jakikolwiek dostęp inżynierski z zewnątrz w celach serwisowych dozwolony jest wyłącznie przez tunel szyfrowany VPN-SSL z wykorzystaniem służbowego sprzętu, po wcześniejszym załogowaniu procedury u Dyrektora lokalizacji.

Faza 5: Dokumentacja Powykonawcza (Wymóg krytyczny)

Przedłożenie dokumentacji niespełniającej wymogów będzie równoznaczne z nieodebraniem prac instalacyjnych. Ze względu na rygor zachowania ciągłości działania, Wykonawca zobowiązany jest dostarczyć ekstremalnie szczegółową dokumentację, na którą składać się muszą m.in.:

1. Zaktualizowana fizyczna i logiczna struktura sieci w ujęciu blokowym (protokoły, media transmisyjne, obiekty).
2. Bezbłędny i wyczerpujący opis wszystkich punktów dystrybucyjnych w obiekcie, w tym numery gniazd na patch-panelach oraz powiązania krosowe z odpowiednimi portami przełączników (wraz z przypisanymi VLAN-ami).
3. Kompletna tablica adresacji: wykaz podsieci LAN i przestrzeni WAN z opisem przeznaczenia i wdrożonym routem.
4. Wykaz wszystkich wdrożonych hostów i systemów wirtualnych uwzględniający: przypisanie do węzłów fizycznych, liczbę rdzeni, parametry dyskowe, pamięć RAM oraz listę oprogramowania.
5. Opracowanie dedykowanego „Rejestru zagrożeń oraz procedur awaryjnych” dla systemu CCTV, określającego kroki ratunkowe, czasy przywrócenia usług oraz macrycę odpowiedzialności.

5. Wymagania gwarancyjne oraz reżim świadczenia usług serwisowych (SLA) dla dostarczonych komponentów:

Poniższe warunki stanowią krytyczny element realizacji zamówienia. Wymaga się od Wykonawcy gotowości do świadczenia zaawansowanego wsparcia technicznego o parametrach klasy Enterprise dla dostarczonych komponentów, przy bezwzględnym zachowaniu procedur bezpieczeństwa Centralnego Ośrodka Sportu.

1. Precyzyjny zakres i czas trwania gwarancji

- Przedmiot gwarancji: Wykonawca udziela pełnej gwarancji wyłącznie na fabrycznie nowe elementy dostarczone w ramach niniejszego postępowania, tj.:
 1. Oprogramowanie do zarządzania systemem monitoringu wizyjnego (VMS) wraz z dostarczonym pakietem licencji (łącznie na 150 kanałów wideo).
 2. Dostarczone i zainstalowane w macierzy Zamawiającego fizyczne dyski twarde.
- Wyłączenia sprzętowe: Gwarancja sprzętowa Wykonawcy nie obejmuje istniejącej infrastruktury Zamawiającego (istniejących kamer, przełączników sieciowych, zapór UTM, serwerów fizycznych, obudowy macierzy Alcatel oraz środowiska VMware). Wykonawca

gwarantuje jednak, że wdrożone przez niego oprogramowanie VMS oraz dostarczone dyski będą w pełni kompatybilne i stabilnie współpracujące z tym środowiskiem.

- Okres gwarancyjny: Na dostarczone oprogramowanie VMS oraz dyski twarde Wykonawca udziela bezwzględnej gwarancji na okres 60 miesięcy (5 lat) od daty podpisania bezusterkowego protokołu odbioru końcowego.

2. Rygorystyczne warunki SLA (Service Level Agreement)

Wykonawca musi zapewnić stałą gotowość do natychmiastowego podjęcia działań naprawczych w przypadku awarii dostarczonych dysków lub krytycznych błędów oprogramowania VMS.

- Czas przystąpienia do usunięcia awarii na miejscu (On-site Response Time): W przypadku zgłoszenia awarii krytycznej (np. padnięcie dysku powodujące degradację macierzy, krytyczny błąd/zatrzymanie usługi VMS uniemożliwiające nagrywanie lub podgląd), Wykonawca jest bezwzględnie zobowiązany do podjęcia prac naprawczych przez autoryzowanego inżyniera bezpośrednio na obiekcie w COS OPO Cetniewo w czasie nie dłuższym niż 12 godzin od momentu skutecznego przesłania zgłoszenia.
- Czas przywrócenia funkcjonalności (Resolution Time): Zgodnie z polityką bezpieczeństwa, w przypadku urządzeń i systemów krytycznych awaria musi zostać usunięta, a pełna funkcjonalność systemu przywrócona najpóźniej w ciągu 48 godzin. W przypadku oprogramowania VMS oznacza to usunięcie błędu, rekonfigurację lub przywrócenie systemu z kopii zapasowej; w przypadku dysków – fizyczną wymianę nośnika i rozpoczęcie przebudowy (rebuildu) macierzy.
- Zarządzanie zmianą: Każda zmiana rekonfiguracyjna w systemie informatycznym dokonana w ramach serwisu musi być nadzorowana i udokumentowana, najlepiej w dzienniku systemu.

3. Procedura obsługi awarii dysków twardych (Procedura "Keep Your Drive")

Z uwagi na fakt, że obszar sieci serwerowej należy uważać za przestrzeń przetwarzania danych osobowych, procedura wymiany uszkodzonych dysków podlega rygorom, od których nie ma żadnych odstępstw:

- Zatrzymanie nośnika: Wymieniane z powodu awarii lub zużycia dyski twarde (pochodzące z puli dostarczonej przez Wykonawcę), na których pracowały systemy COS, bezwzględnie pozostają własnością Zamawiającego.
- Fizyczna utylizacja: Dyski przeznaczone do likwidacji są na miejscu demontowane i podlegają udokumentowanej utylizacji przeprowadzanej przez Zamawiającego. Wykonawca musi uwzględnić ten fakt (brak zwrotu uszkodzonego nośnika w procesie RMA) w wycenie swojej oferty.

4. Wymogi bezpieczeństwa podczas interwencji serwisowych

Każda interwencja inżyniera (zarówno przy fizycznej wymianie dysku, jak i pracach w konsoli VMS) podlega surowym procedurom Ośrodka:

- Dostęp zdalny (próba diagnozy przed upływem 12h): Jeżeli Wykonawca zechce dokonać wstępnej diagnozy oprogramowania VMS zdalnie, jest to możliwe wyłącznie za pośrednictwem aplikacji tworzącej tunel szyfrowany VPN-SSL. Decyzję o przyznaniu takiego dostępu wydaje każdorazowo Dyrektor lokalizacji COS. Wszystkie dostępy tego typu muszą być precyzyjnie ewidencjonowane, opisane i uzasadnione.
- Protokołowany dostęp do poświadczeń: W przypadku konieczności użycia haseł administracyjnych przechowywanych w tzw. "bezpiecznych kopertach" (np. do restartu maszyny wirtualnej, na której stoi VMS), wymagana jest informacja w postaci protokołu – kto, kiedy i z jakiej przyczyny użył hasła.

- Rotacja poświadczeń: Po zakończeniu interwencji serwisowej przez Wykonawcę, użyte hasło z "bezpiecznej koperty" musi zostać niezwłocznie zmienione w celu zachowania rozliczalności i ponownie w niej umieszczone.