**Załącznik nr 7 do SWZ - OPIS PRZEDMIOTU ZAMÓWIENIA**

Zakres zamówienia:

1. Dostawa i konfiguracja stanowiska wizualizacji (ul. Akademicka 3, Centrum Monitoringu) w postaci:

- 2 stacji roboczych,

- 2 monitorów 50" (rozdzielczość 4K, możliwość pracy 24/7),

- serwera zarządzającego,

- serwera SIP (- porty FXS - minimum 6, - porty FXO - minimum 6, - jednoczesna liczba połączeń - minimum 400, - minimalna ilość użytkowników – 3000, - minimalna ilość pokoi konferencyjnych – 6, - peryferia – minimum 2 x USB 3.0),

- rejestratora CCTV (- minimum 32 kanały IP do rozdzielczości 32 mpx, - obsługa funkcji AI, - miejsce na minimum 3 dyski HDD). Rejestrator należy doposażyć w minimum 3 dyski HDD   
o minimalnej pojemności 14 TB,

- szafa stojąca rack o minimalnych wymiarach 1000x800x2000 mm (minimum 40U).

2. Dostawa, montaż 6 kamer CCTV (min. rozdz. 5 mpx, PoE, kąt widzenia minimum ~109O)   
w pomieszczeniach technicznych Centrum Futuri,

3. Wykonanie integracji instalacji KD, CCTV, SSWIN, SSP dla Centrum Futuri (ul. Waszyngtona 15 B, 15 C), w tym: 45 kamer CCTV, 68 czujek systemu SSWiN, 407 czujek systemu SSP, 93 przejścia KD oraz szlaban wjazdowo / wyjazdowy, depozytor kluczy,

4. Dostawa, montaż, integracja z systemem KD depozytora kluczy (min. 32 gniazda, z ekranem dotykowym oraz czytnikiem 13,56 MHz) dla Centrum Futuri,

5. Dostawa, montaż 3 szt. videodomofonów zewnętrznych (min. rozdz. 2 mpx, PoE, kąt widzenia nie mniejszy niż 120O, z możliwością wybrania dowolnego nr wewnętrznego Zamawiającego   
z klawiatury numerycznej), 1 szt. monitora do videodomofonu (pojemnościowy ekran dotykowy IPS, o rozdzielczości nie mniejszej niż 1024x600, PoE, z możliwością otwarcia elektrozamka) oraz wykonanie integracji z istniejącym systemem łączności VoIP budynku Centrum Futuri wraz z możliwością komunikacji z Centrum Monitoringu,

6. Dostawa, montaż 6 szt. kamer CCTV dla Collegium Floridum (min. rozdz. 5 mpx, PoE, kąt widzenia ~109O) (ul. Mickiewicza 2 B),

7. Wykonanie integracji instalacji KD, CCTV, SSWIN, SSP dla Collegium Floridum (ul. Mickiewicza 2 B) w tym: 8 kamery CCTV, 40 czujek systemu SSWiN, 178 czujek systemu SSP, 27 przejścia KD.

Projektowany system monitorowania i wizualizacji ma umożliwić użytkownikowi końcowemu zarządzanie stanami oraz zdarzeniami, które zostają wykryte przez różne systemy bezpieczeństwa, tworząc jednolity plan sytuacyjny dla zespołu obiektów.

Zastosowanie integracji systemów bezpieczeństwa ma na celu znaczące obniżenie kosztów utrzymania i eksploatacji systemów poprzez:

• Zcentralizowanie i zautomatyzowanie procesu detekcji sytuacji alarmowych;

• Ograniczenie liczby kadry pracowniczej wewnętrznej lub zewnętrznej odpowiedzialnej za monitorowanie systemów bezpieczeństwa;

• Ograniczenie kosztów ewentualnych działań serwisowych.

Platforma zarządzania musi umożliwiać wzajemne współdziałanie poniższych podsystemów za pomocą interfejsów programowych, które mogą być dodawane zapewniając skalowalność systemu:

• Systemy sygnalizacji pożaru (SSP) – w tym Polon 4000, Polon 6000;

• Systemy sygnalizacji włamania i napadu (SSWiN) – w tym Satel Integra;

• System kontroli dostępu (SKD) – w tym system RACS-5 ROGER;

• System telewizji dozorowej (CCTV) – w tym systemy BCS Line, BCS Point, Dahua, Hikvision, Bosch

i inne;

• System depozytorów kluczy – w tym systemy firmy Roger.

Projektowany system ma zapewnić:

• Dostarczenie wymaganego zestawu informacji zarządczych z systemów bezpieczeństwa;

• Wsparcie wypracowania właściwej decyzji w możliwie najkrótszym czasie;

• Automatyzację podejmowanych działań w oparciu o zatwierdzone procedury, zgodne z przyjętą polityką bezpieczeństwa;

• Archiwizowanie działań i operacji podejmowanych przez operatorów, celem weryfikacji jak   
i optymalizacji procesów oraz procedur;

• Nadzór nad infrastrukturą i optymalizacja kosztów utrzymania (serwisowania).

Wymagania dla projektowanej platformy :

• Ma być neutralna względem integrowanych systemów;

• Ma być obsługiwana przez dedykowaną aplikację kliencką, wykonaną w technologii okienkowej;

• Niedopuszczalne jest zastosowanie przeglądarki internetowej i technologii okien pop-up, celem eliminacji możliwości przechwycenia danych;

• Ma zapewniać możliwość zdefiniowania hierarchii lokalizacji (map), celem uporządkowanego administrowania danych z monitorowanych systemów;

• Powinna zapewniać możliwość pracy w tle, co oznacza iż na stacji roboczej można opcjonalnie używać innych aplikacji, a w momencie wystąpienia zdarzenia / alarmu, głownie okno aplikacji przesunie się na wierzch. Alarm zostanie zasygnalizowany dodatkowo akustycznie oraz optycznie;

• Ma zapewniać szyfrowanie komunikacji z kontrolerami KD co najmniej na poziomie bezpieczeństwa, jaki zapewnia algorytm AES128 CBC;

• Musi zapewniać możliwość zarządzania Użytkownikami systemu KD i uwierzytelniania operatorów za pośrednictwem usługi Active Directory;

• Powinien zapobiegać przedostawaniu się danych i poleceń do systemu z zewnątrz bez uzasadnienia, a także uniemożliwiać osobom trzecim dostęp do systemu. W ten sposób połączenia IP między serwerami i klientami będą szyfrowane przez TLS 1.2;

• Ma być dostępna w polskiej wersji językowej.

Platforma zarządzająca musi być zaprojektowana tak, aby umożliwiała centralnie kontrolowaną interakcję między systemami bezpieczeństwa budynku, jak i zarządzanie informacjami, jednak nie może zastępować żadnego zainstalowanego pojedynczego systemu.

Okno systemu zarządzania bezpieczeństwem musi obejmować:

• Drzewko nawigacyjne z listą map

• Monitor map

o Podkład graficzny w formacie rastrowym (BMP, JPEG), wektorowym (SVG) lub import z formatu AutoCad ( DWG, DXF);

o Na podkładzie muszą być umieszczane interaktywne obiekty (czujki, przejścia, kamery);

o Obiekty muszą prezentować swoje aktualne stany;

o Musi być możliwe wydawanie poleceń obiektom (otwarcie przejście, odtworzenie obrazu z kamery).

• Monitor powiadomień (stos alarmowy) prezentujący listę posortowanych alarmów, powiadomień i awarii;

Aplikacja musi umożliwiać wizualizację następujących funkcjonalności międzysystemowych (KD, CCTV, SSWiN itd.) za pomocą dodawania odpowiednich licencji i / lub podnoszenia wersji w przypadku dodawania nowych systemów składowych.

• Wizualizacja stanu drzwi (zamknięte / otwarte) objętych kontrolą dostępu;

• Wizualizacja stanów czytnika, kontaktronu;

• Wizualizacja stanów poszczególnych elementów detekcyjnych (np. czujek ruchu PIR);

• Zazbrajanie i rozbrajanie poszczególnych stref SSWiN;

• Wywołanie okna widoku kamery CCTV w sytuacjach alarmowych wywołanych przez system KD, SSWiN, SSP, depozytor;

• Kliknięcie ikony kamery ma spowodować wyświetlenie obrazu z danej kamery / videodomofonu;

• Dla kamer PTZ, pełna możliwość sterowania kamerą z poziomu mapy;

• Stan poszczególnych stref systemów SSP oraz SSWiN musi być wizualizowany na mapach z wykorzystaniem ikon oraz map o dowolnie kształcie odwzorowującym faktyczny obszar danej strefy;

• Monitor powiadomień musi przedstawiać bieżące powiadomienia z podziałem na 4 zakładki: SSP, SSWiN, KD oraz awarie;

• Powiadomienia muszą być wyświetlane w kolejności według ich priorytetu. Ponadto, konieczne jest zapewnienie możliwości lokalizacji powiadomień na mapach;

• Rejestr powiadomień musi umożliwić przegląd i filtrowanie powiadomień zarejestrowanych w systemie, obejmujących kategorie: alarmu, ostrzeżenia, informacje oraz awarie;

• System musi umożliwić uruchomienie monitora telewizji dozorowej, prezentującego zbiorczy obraz z kamer w wybranym układzie;

• System musi wyświetlać stany alarmowe oraz stany awaryjne, zapewniając jednocześnie czytelne wskazanie kolorystyczne stanu danego przejścia i urządzenia;

• System musi umożliwiać sterowanie każdym z przejść, włączając w to funkcje takie jak otwarcie, zablokowanie, blokady czasowe, odblokowania czasowe itp;

• System musi umożliwiać ustawienia harmonogramów czasowych otwarcia przejść, zapewniając elastyczne zarządzanie czasem dostępu;

• System musi umożliwiać przypisywanie uprawnień dla kart dostępu oraz blokowanie kart dostępu w przypadku potrzeby;

• System powinien umożliwiać zarządzanie użytkownikami depozytora kluczy oraz blokowanie wyjścia Zamawiającego z obiektu bez zwrócenia klucza do depozytora;

• System musi umożliwiać generowanie raportów dla użytkowników, przejść, stref oraz innych elementów, umożliwiając pełne monitorowanie i analizę działania systemu.

Dla ułatwienia pracy administratora przy stacji operatorskiej należy zainstalować czytnik administratora z interfejsem USB pozwalający na programowanie kart dostępu.

Ponadto projektowana platforma musi spełniać poniższe wymogi.

• Aplikacja musi pozwalać na definiowanie nieograniczonej liczby operatorów, chronionych hasłem dostępu;

• Aplikacja musi zapewniać możliwość zdefiniowania nieograniczonej liczby ról operatorów. Role mają określać wygląd i funkcje dostępne z poziomu interfejsu systemu;

• Aplikacja musi umożliwiać przypisanie kilku ról jednemu operatorowi;

• Prawa dostępu i obsługi powinny być przypisane do poszczególnych ról, a następnie propagowane na operatorów;

• Aplikacja musi integrować się z systemem rejestracji obrazu telewizji przemysłowej za pośrednictwem interfejsu API danego producenta lub ONVIF;

• Aplikacja musi zapewniać wyświetlanie obrazu z dowolnych kamer (analogowe i cyfrowe), w tym samym formacie w ramach interfejsu Zamawiającego;

• Aplikacja musi zapewniać wyświetlenie obrazu z kamery w ramach menadżera video (modułu CCTV), poprzez funkcję drag & drop, wybór ekranu w ramach układu i wybór kamery z mapy;

• Aplikacja musi zapewniać automatyczne wyświetlenie kamery w odpowiedniego obszaru („obraz na żywo”);

• Aplikacja musi zapewniać wyświetlanie wielu strumieni w ramach jednego interfejsu Zamawiającego, w tym w kilku definiowalnych bądź wybranych układach;

• Aplikacja musi zapewniać możliwość eksportu fragmentu strumienia z kamery, jako „klipu”

z systemu CCTV i jego zapisanie w archiwum wideo;

• Aplikacja musi posiadać centralny stos alarmów, z możliwością jego dostosowywania do potrzeb Zamawiającego;

• Aplikacja musi zapewniać akustyczną i optyczną sygnalizację przychodzących zdarzeń;

• Aplikacja musi zapewniać wyświetlenie, w zależności od typu zdarzenia procedurę postępowania oraz informacje powiązane;

• Aplikacja musi zapewniać możliwość informowania o wystąpieniu określonego typu zdarzenia za pomocą sms’a oraz mailem;

• Aplikacja musi zapewniać możliwość definiowania czasu koniecznego na potwierdzenia zdarzenia przez operatora i automatycznie informować w przypadku braku reakcji ze strony operatora.

W zakresie graficznego interfejsu Zamawiającego (GUI) platforma musi spełniać następujące wymagania:

• Aplikacja musi mieć zintegrowany graficzny interfejs Zamawiającego (GUI), który zapewni użytkownikom wygodne i intuicyjne korzystanie z systemu;

• Aplikacja musi umożliwiać wyświetlanie wielu treści jednocześnie, takich jak mapy, monitory, przyciski, pasek narzędziowy, stos zdarzeń i alarmów oraz inne elementy, aby operator mógł efektywnie monitorować i zarządzać systemem;

• GUI aplikacji nie może ograniczać liczby wyświetlanych jednocześnie okien ani definiowanych widoków, co pozwoli użytkownikom dostosować interfejs do swoich potrzeb i preferencji;

• Aplikacja musi być wyposażona w edytor graficzny umożliwiający tworzenie własnych ikon dla elementów na mapach, co pozwoli na lepszą personalizację interfejsu i łatwiejsze zrozumienie informacji przez operatorów;

• Dodatkowo, aplikacja powinna zawierać podstawową bibliotekę ikon do różnych przypadków użycia, co ułatwi szybkie projektowanie interfejsu i zapewni spójność wizualną;

• Aplikacja musi umożliwiać wstawianie na mapach przycisków z przypisanymi komendami, co pozwoli operatorom szybko wykonywać określone akcje bez konieczności przemieszczania się po różnych ekranach;

• Ponadto, aplikacja musi zapewniać możliwość definiowania warstw, co pozwoli na logiczne grupowanie określonych typów informacji, na przykład punktów danych, co ułatwi zarządzanie danymi i poprawi czytelność interfejsu.

Minimalne wymagania, które system musi spełniać na etapie pierwszego wdrożenia:

• Możliwa do rozbudowy licencja bazowa służąca do administrowania i przetwarzania zdarzeń z poziomu stacji roboczej

• Możliwość rozbudowy o dodatkowe stacje robocze.

• 1 natywny wbudowany operator

System musi cechować się skalowalnością i elastycznością, aby dostosować się do zmieniających się potrzeb i architektury systemów na obiekcie. Zapewnia to niezawodność oraz możliwość rozwoju   
o nowe funkcje. Oto kluczowe funkcje, które system musi zapewnić:

• Obsługa interfejsów bez limitów: System powinien być zdolny do obsługi różnorodnych interfejsów dla systemów bez żadnych ograniczeń ilościowych. Dzięki temu możliwe będzie integracja z nowymi systemami oraz rozwój funkcjonalności.

• Możliwość tworzenia interfejsów: W przypadku braku gotowych interfejsów, system musi umożliwiać tworzenie własnych interfejsów, co pozwoli na integrację z niestandardowymi systemami.

• Obsługa Punktów Danych (DPU) bez limitu: System powinien umożliwiać obsługę punktów danych bez ograniczeń ilościowych, zapewniając elastyczność w gromadzeniu i przetwarzaniu danych.

• Brak limitu ilości operatorów: System musi umożliwiać nadanie ilości operatorów bez żadnych ograniczeń, co pozwoli na swobodne zarządzanie dostępem i kontrolę systemu przez różnych użytkowników.

• Licencja na rozszerzenie funkcji klienta "natywnego" o moduł wideo: System powinien oferować możliwość rozbudowy funkcji klienta "natywnego", który umożliwi wyświetlanie i sterowanie różnymi systemami wideo. Dzięki temu operatorzy będą mieli kompleksowy dostęp do monitoringu wideo.

• Tryb wielu monitorów: System powinien wspierać tryb wielu monitorów, który umożliwi rozszerzenie wyświetlania interfejsów na kilka monitorów. Pozwoli to operatorom na lepszą organizację pracy i łatwiejszy dostęp do potrzebnych informacji.

W zakresie archiwizacji, system musi spełniać następujące wymogi:

• Pełna archiwizacja przetwarzanych zdarzeń: System musi zapewniać pełną archiwizację przetwarzanych zdarzeń, co pozwoli na śledzenie historii oraz analizę danych w celu lepszego zrozumienia sytuacji i podejmowania decyzji.

• Możliwość filtrowania rejestru zdarzeń: Aplikacja powinna umożliwiać filtrowanie rejestru zdarzeń za pomocą konfigurowalnych filtrów, co ułatwi wyszukiwanie konkretnych informacji i skróci czas analizy danych.

System musi zapewniać nieograniczoną licencyjnie ilość jednoczesnych połączeń klienckich   
z komputerów zdalnych wyposażonych w aplikacje kliencką systemu.

Podane poniżej zalecenia mają charakter informacyjny. Komputery PC powinny być dobierane   
w zależności od wielkości systemu.

Wymagania serwer:

System operacyjny z rodziny Windows lub równoważny (załącznik nr 3) z pakietem MS .NET Framework 4.8.

Wymagania:

• RAM: min. 32 GB (64 GB dla dużych systemów, pow. 50 kontrolerów)

• CPU: Intel Core i7 lub równoważny (Core i9 dla dużych systemów pow. 50 kontrolerów.)

• Karta graficzna: dedykowana, min. 4GB pamięci VRAM

• Zalecana rozdzielczość ekranu: min. 1920x1080

Serwerowa baza danych np. MS SQL Standard lub równoważna (załącznik nr 3)

Wymagania klient:

• System operacyjny z rodziny Windows lub równoważny (załącznik nr 3) z pakietem MS .NET Framework 4.8.

• RAM: min. 16 GB (32 GB dla dużych systemów, pow. 50 kontrolerów)

• CPU: Intel Core i7 lub równoważny (Core i9 dla dużych systemów pow. 50 kontrolerów.)

• Karta graficzna: dedykowana, min. 4GB pamięci VRAM, obsługująca co najmniej 4 monitory

• Zalecana rozdzielczość ekranu: min. 1920x1080

Zamawiający w przedmiocie zamówienia wskazał oprogramowanie typu:

1. Windows 10 lub równoważny (licencja komercyjna),

2. Baza danych MS SQL

**Zamawiający określa zakres równoważności:**

**Ad.1 Windows 10**

- Licencja na zaoferowany system operacyjny musi być w pełni zgodna z warunkami licencjonowania producenta oprogramowania,

- Interfejsy Zamawiającego dostępne w kilku językach do wyboru – minimum w Polskim i Angielskim,

- Udostępnianie modemu,

- Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6,

- Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,

- Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych

- Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,

- Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),

- Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,

- Możliwość pracy w domenie i kontrola użytkowników w technologii Active Directory, scentralizowane zarządzanie oprogramowaniem i konfigurację systemu w technologii Group Policy.

- Mechanizmy logowania w oparciu o: 1. Login i hasło,

2. Karty z certyfikatami (smartcard),

3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),

- Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,

- Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,

- Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników,

- Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);

- Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi,

- Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny,

- Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,

- Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk,

- Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,

- Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,

- Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego Zamawiającego celem rozwiązania problemu z komputerem,

- Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,

- Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,

- Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe,

- Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,

- Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,

- Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),

- Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),

- Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,

- Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,

- Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.

- Możliwość nieodpłatnego instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu,

- Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,

- Zintegrowany z systemem, moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez Zamawiającego module indeksacji zasobów lokalnych,

- Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym.

**Ad.2 Baza danych MS SQL Standard**

Zamawiający dopuszcza możliwość dostawy licencji oprogramowania równoważnego,

o parametrach nie gorszych niż wskazane, o ile będzie to oprogramowanie w pełni zgodne i kompatybilne z oprogramowaniem Centrum Monitoringu Uniwersytetu Medycznego w Białymstoku oraz będzie spełniało poniższe wymagania minimalne:

a) Oprogramowanie silnika baz danych przeznaczone do instalacji w ramach lokalnej infrastruktury sprzętowej i programowej posiadanej przez Zamawiającego. Silnik zostanie zainstalowany na serwerze Microsoft Windows Server Standard lub alternatywnie instancja zgodnego systemu operacyjnego dostarczonego przez Wykonawcę wraz z silnikiem baz danych może być zainstalowana na maszynie wirtualnej działającej pod kontrolą Microsoft Hyper-V (rola serwera Windows Server Standard),

b) Ilość oferowanych licencji oprogramowania silnika baz danych musi zapewnić wykorzystanie mocy obliczeniowej min. 8 rdzeni procesora oraz min. 32 GB pamięci RAM,

c) Ilość oferowanych licencji oprogramowania silnika baz danych musi umożliwiać pełne wykorzystanie silnika dla użytkowników z nieograniczonej puli stanowisk dostępowych,

d) Zarządzanie silnikiem baz danych dostępne będzie z poziomu narzędzia graficznego (aplikacja typu desktop lub aplikacja obsługiwana w przeglądarce WWW). Wszystkie funkcje zarządzania muszą być dostępne lokalnie bez wymaganego dostępu do sieci Internet. Narzędzie graficzne do zarządzania silnikiem musi zapewniać możliwość zarządzania i konfiguracji wszystkich usług implementowanych przez silnik baz danych.

e) Dostępna funkcja profilowania silnika baz danych, rejestrująca określone wg filtra zapytania spływające do silnika baz danych w czasie rzeczywistym w formie dziennika zdarzeń, której zadaniem będzie identyfikacja ewentualnych problemów lub błędów w działaniu aplikacji,

f) Zarządzanie silnikiem baz danych dostępne będzie z poziomu narzędzia linii poleceń umożliwiające automatyzację czynności administracyjnych, min.:

a. Wykonywanie zadań kopii zapasowych,

b. Zarządzanie kontami użytkowników,

c. Zarządzanie uprawnieniami użytkowników,

d. Zarządzanie pracą silnika baz danych (min. akcje uruchomienia i zatrzymania pracy silnika),

e. Wykonywanie zapisanych skryptów poleceń SQL z obsługą

przekierowywania wyjścia na standardowe wyjście konsoli lub do pliku,

g) Obsługa aktualizacji automatycznych dla silnika musi umożliwiać automatyczne ściąganie i instalację poprawek bezpieczeństwa producenta oprogramowania dla minimalizacji zagrożeń powodowanych przez wykryte luki w zabezpieczeniach oprogramowania silnika,

h) Silnik baz danych musi posiadać mechanizm pozwalający na duplikację określonych baz danych między dwiema instancjami, zapewniający replikację danych w czasie rzeczywistym,

i) Silnik baz danych musi obsługiwać mechanizm kompresji kopii zapasowych w trakcie ich tworzenia,

j) Obsługa automatycznego szyfrowania kopii zapasowych baz danych (w trakcie wykonywania) przy użyciu min. funkcji kryptograficznej AES-256 z użyciem klucza asymetrycznego. Możliwość szyfrowania kopii zapasowych baz danych niezaszyfrowanych,

k) Wsparcie dla zastosowanych reguł bezpieczeństwa, min. zastosowanie mechanizmu weryfikacji dostatecznego poziomu długości i komplikacji haseł użytkowników, możliwość zintegrowania uwierzytelniania użytkowników z Active Directory,

l) Automatyczne rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym o następujących cechach:

a. Zredukowany do minimum negatywny wpływ logowania na wydajność silnika baz danych,

b. Możliwość selektywnego wybierania rejestrowanych zdarzeń takich jak: monitorowanie stanu obciążenia silnika, operacje odczytu i zapisu danych na dysku, przekroczenie czasu wykonywania operacji, aktywność Zamawiającego,

m) Możliwość definiowania nowych typów danych przechowywania z obsługą danych hierarchicznych. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Wykonawcę języku programowania,

n) Obsługa danych w formacie XML w zakresie umożliwiającym składowanie i obróbkę danych w postaci struktur XML. Silnik musi zapewniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli oraz zapewnić mechanizm do walidacji struktur XML wykorzystując szablony XSD. Ponadto silnik musi udostępniać język zapytań zgodny ze standardem XQuery do obsługi struktur XML,

o) Obsługa tworzenia funkcji i procedur w innych językach programowania z możliwością ich uruchomienia z poziomu zapytań SQL lub wyzwalaczy SQL Trigger.