Załącznik nr 1.1 do OPZ

na dostawę i instalację infrastruktury teleinformatycznej

Specyfikacja przedmiotu zamówienia

Zamawiający - Partner nr 06

Instytut Gruźlicy i Chorób Płuc Oddział Terenowy w Rabce-Zdrój

część zamówienia – sprzęt serwerowo-sieciowy

w projekcie ,,Wprowadzenie nowoczesnych e-Usług w podmiotach leczniczych nadzorowanych przez Ministra Zdrowia”

MIEJSCE DOSTAWY:

ul. Prof. Jana Rudnika 3b

34-721 Rabka Zdrój

W poniższej tabeli przedstawiono typy oraz liczbę zamawianej infrastruktury teleinformatycznej.

Tabela 1. Typy oraz liczba zamawianej infrastruktury teleinformatycznej.

Lp.	Typ	Zamówienie podstawowe: Liczba zamawianego sprzętu (sztuk)	Zamówienie opcjonalne: Liczba zamawianego sprzętu (sztuk)	Zamówienie łączne
Zamówienie podstawowe:				
1.	Baza danych	1	Zamawiający nie przewiduje skorzystania z prawa opcji	1
2.	Serwer backupowy	1		1
3.	Przełącznik dystrybucyjny	9		9
4.	Moduły SFP+ do przełączników dystrybucyjnych typ 1	14		14
5.	Moduły SFP+ do przełączników dystrybucyjnych typ 2	4		4
6.	Biblioteka taśmowa	1		1
7.	Punkt dostępowy Wifi	15		15
8.	UTM	2		2
9.	Szafa serwerowa	1		1
10.	Licencja dostępowa	30		30
11.	Oprogramowanie backupowe	1		1
12.	Przełącznik SAN	2		2

W poniższej tabeli przedstawiono szczegóły dotyczące planowanej do zamówienia infrastruktury teleinformatycznej – specyfikacja przedmiotu zamówienia.

Tabela 2. Szczegóły zamawianej infrastruktury teleinformatycznej w podziale na komponenty.

1. Baza danych

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
Baza danych – specyfikacja przedmiotu zamówienia		
1.	Licencje bazy danych	1) Dostępność oprogramowania na współczesne 64-bitowe platformy Unix (HP-UX dla procesorów Itanium, Solaris dla procesorów SPARC i Intel/AMD, IBM AIX dla procesorów POWER, Intel/AMD Linux, MS Windows). Identyczna funkcjonalność serwera bazy danych na ww. platformach 2) Dostarczone licencje nie mogą ograniczać liczby użytkowników końcowych korzystających z oprogramowania ani liczby przetwarzanych lub przechowywanych dokumentów, plików, rekordów, żądań, etc. Licencje nie mogą być ograniczone czasowo. 3) Proponowany zestaw licencji powinien być jednorodny. Wymagana jest dostawa oprogramowania certyfikowanego pod względem zgodności ze sobą. Wymaganie obejmuje: 4) Oprogramowanie bazy danych ze względu na zgodność z systemem operacyjnym oraz platformą sprzętową, 5) Systemy operacyjne używane do uruchamiania serwerów bazy danych ze względu na zgodność z platformą sprzętową. 6) Dostępność narzędzi migracji baz danych pomiędzy platformami na poziomie fizycznym (kopiowanie / konwersja plików danych) oraz logicznym (narzędzia eksportu / importu), wymaganie nie musi zostać spełnione w przypadku dostarczenia oprogramowania działającego w oparciu o jedną bazę danych. 7) Oprogramowanie klienckie, za pomocą, którego można łączyć się do bazy danych musi być dostępne na wielu platformach systemowo-sprzętowych (minimalny zakres platform taki jak dla oprogramowania serwera bazy danych) 8) Wsparcie protokołu XA. 9) Wsparcie standardu JDBC 3.0. 10) Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym. 11) Wbudowana obsługa wyrażeń regularnych zgodna ze standardem POSIX dostępna z poziomu języka SQL jak i procedur/funkcji składowanych w bazie danych. 12) RDBMS musi zapewniać niezależność platformy systemowej dla oprogramowania klienckiego od platformy systemowej bazy danych. 13) RDBMS musi zapewniać przetwarzanie transakcyjne wg reguł ACID z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności. Mechanizm izolowania transakcji musi pozwalać na spójny odczyt modyfikowanego obszaru danych bez wprowadzania blokad, spójny odczyt nie może blokować możliwości wykonywania zmian. 14) RDBMS musi posiadać możliwość zagnieżdżania transakcji – Możliwość uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej. 15) Dostępność poziomu serializowanego poziomu izolowania transakcji (Serializable). 16) Możliwość zmiany domyślnego trybu izolowania transakcji (Read Commited) na inny (Read Only, Serializable) za pomocą komend serwera bazy danych. 17) Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode) zarówno po stronie serwera bazy danych jak i oprogramowania klienckiego. Wsparcie dla polskich stron kodowych – ISO-8859-2, MS Win-

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		dows Code Page 1250 oraz PC 852. Automatyczna konwersja znaków pomiędzy różnymi ustawieniami stron kodowych po stronie klienta i serwera bazy danych. 18) Możliwość migracji bazy danych utrzymujących dane znakowe w 8-bitowej stronie kodowej do Unicode. 19) Możliwość definiowania w przestrzeni danych (plików) dla danych użytkownika obszarów o innym niż domyślny rozmiarze bloku. 20) Możliwość bez dodatkowych ograniczeń przechowywania wierszy, których rozmiar przekracza rozmiar bloku bazy danych. 21) Możliwość budowania indeksów o strukturze B-drzewa. Baza danych powinna umożliwiać założenie indeksu jednej lub większej liczbie kolumn tabeli, przy czym ograniczenie liczby kolumn, na których założony jest 1 indeks nie powinno być mniejsze niż 16. 22) Możliwość budowania widoków zmaterializowanych odzwierciedlających stan danych zdefiniowanych przez zapytanie SQL. Widok zmaterializowany przechowuje rezultat zapytania, którego aktualizacja odbywa się w jednej z dostępnych strategii – na żądanie, okresowo bądź po każdym zatwierdzeniu transakcji modyfikującej tabele, na której oparty jest widok zmaterializowany. 23) Możliwość szybkiego odświeżania danych w widoku zmaterializowanym na podstawie mechanizmu identyfikacji zmian w danych źródłowych. 24) Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy). 25) Kosztowy model optymalizacji instrukcji SQL. 26) Model statystyk optymalizatora kosztowego musi pozwalać na odwzorowanie nierównomierności rozkładu danych (składowanie informacji o rozkładzie wartości występujących w kolumnach za pomocą histogramu bądź porównywalnego funkcjonalnie modelu odwzorowania). 27) Możliwość uwzględnienia korelacji wartości występujących w niezależnych kolumnach tabeli w modelu statystyk optymalizatora kosztowego. 28) RDBMS powinien umożliwiać wskazywanie optymalizatorowi SQL preferowanych metod optymalizacji na poziomie konfiguracji parametrów pracy serwera bazy danych oraz dla wybranych zapytań. Powinna istnieć Możliwość umieszczania wskazówek dla optymalizatora w wybranych instrukcjach SQL. 29) Wsparcie dla procedur i funkcji składowanych w bazie danych. Język programowania powinien być językiem proceduralnym, blokowym (umożliwiającym deklarowanie zmiennych wewnątrz bloku), oraz wspierającym obsługę wyjątków. W przypadku, gdy wyjątek nie ma zadeklarowanej obsługi wewnątrz bloku, w razie jego wystąpienia wyjątek powinien być automatycznie propagowany do bloku nadrzędnego bądź wywołującej go jednostki programu. 30) Procedury i funkcje składowane powinny mieć Możliwość parametryzowania za pomocą parametrów prostych jak i parametrów o typach złożonych, definiowanych przez użytkownika. Funkcje powinny mieć Możliwość zwracania rezultatów jako zbioru danych, możliwego do wykorzystania jako źródło danych w instrukcjach SQL (czyli występujących we frazie FROM). Ww. jednostki programowe powinny umożliwiać wywoływanie instrukcji SQL (zapytania, instrukcje DML, DDL), umożliwiać jednoczesne otwarcie wielu tzw. kursorów pobierających paczki danych (wiele wierszy za jednym pobraniem) oraz wspierać mechanizmy transakcyjne (np. zatwierdzanie bądź wycofanie transakcji wewnątrz procedury). 31) Możliwość kompilacji procedur składowanych w bazie do postaci kodu binarnego (biblioteki dzielonej).

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		32) W przypadku, gdy w wyzwalaczu na poziomie instrukcji DML wystąpi błąd zgłoszony przez motor bazy danych bądź ustawiony wyjątek w kodzie wyzwalacza, wykonywana instrukcja DML musi być automatycznie wycofana przez serwer bazy danych, zaś stan transakcji po wycofaniu musi odzwierciedlać chwilę przed rozpoczęciem instrukcji, w której wystąpił ww. błąd lub wyjątek. 33) Możliwość wykonania równoczesnych operacji DML (Insert/Update/Delete) na tej samej tabeli. 34) Powinna istnieć Możliwość autoryzowania użytkowników bazy danych za pomocą rejestru użytkowników założonego w bazie danych bądź mechanizmu zewnętrznego w stosunku do bazy danych. 35) Przywileje użytkowników bazy danych powinny być określane za pomocą przywilejów systemowych (np. prawo do podłączenia się do bazy danych - czyli utworzenia sesji, prawo do tworzenia tabel itd.) oraz przywilejów dostępu do obiektów aplikacyjnych (np. odczytu / modyfikacji tabeli, wykonania procedury). Baza danych powinna umożliwiać nadawanie ww. przywilejów za pośrednictwem mechanizmu grup użytkowników / ról bazodanowych. W danej chwili użytkownik może mieć aktywny dowolny podzbiór nadanych ról bazodanowych. 36) Możliwość wykonywania i katalogowania kopii bezpieczeństwa bezpośrednio przez serwer bazy danych. Możliwość zautomatyzowanego usuwania zbędnych kopii bezpieczeństwa przy zachowaniu odpowiedniej liczby kopii nadmiarowych - stosownie do założonej polityki nadmiarowości backup'ów. Możliwość integracji z powszechnie stosowanymi systemami backupu (Legato, Veritas, Tivoli, itp.). Wykonywanie kopii bezpieczeństwa powinno być możliwe w trybie offline oraz w trybie online(hot backup). 37) Odtwarzanie powinno umożliwiać odzyskanie stanu danych z chwili wystąpienia awarii bądź cofnąć stan bazy danych do punktu w czasie. W przypadku odtwarzania do stanu z chwili wystąpienia awarii odtwarzaniu może podlegać cała baza danych bądź pojedyncze pliki danych. 38) Możliwość uruchomienia bazy danych w środowisku klastra wielu aktywnych serwerów bazy danych. 39) Zwiększenie bądź zmniejszenie liczby serwerów obsługujących klastrową bazę danych nie może powodować konieczności reorganizacji fizycznej bazy danych (struktura plików danych). 40) Zwiększenie bądź zmniejszenie liczby serwerów obsługujących klastrową bazę danych nie może powodować konieczności reorganizacji logicznej struktury baz danych (tabel / indeksów). 41) Unieruchomienie jednego z serwerów klastra bazy danych nie może powodować braku dostępu do jakiejkolwiek części danych – baza danych musi być nadal dostępna za pośrednictwem funkcjonujących dalej serwerów. 42) Możliwość kontynuacji pracy użytkowników podłączonych do serwera klastrowej bazy danych, który uległ awarii. Wymagana jest Możliwość przeniesienia sesji na inny serwer oraz automatycznego powiadomienia aplikacji o wykonaniu przełączenia. 43) Każdy z serwerów klastra musi mieć Możliwość uspójnienia lub odtworzenia całej bazy danych w sytuacji awarii nośników lub nagłego zatrzymania innego serwera, który utrzymywał w buforze bazy danych zmodyfikowane, ale niezapisane bloki danych. 44) Obraz bazy danych (metadane, obiekty bazy danych, stan danych) w klastrowej bazie danych musi być niezależny od serwera, do którego zostało nawiązane połączenie.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		45) Część funkcjonalna lub rozszerzenie serwera bazy danych, musi działać na platformach sprzętowych i systemowych wspieranych przez bazę danych; pozwalająca na uruchomienie bazy w środowisku klastra wielu aktywnych serwerów bazy danych. 46) Dopuszcza się istnienie dodatkowej przestrzeni tabel w ramach instalacji, w której użytkownik będzie mógł przechowywać dane zapytań, własne procedury, funkcje, tabele itp. Dopuszczalne będzie odpytywanie wykorzystywanej bazy danych. 47) Licencja bazy danych jest bezterminowa. Prawa do aktualizacji wygasają po upływie 3 lat od daty zakupu. Możliwość przedłużenia gwarancji.
2.	Instalacja, konfiguracja i migracja danych	1) Realizacji usługi zgodnie z wymogami licencyjnymi producenta dostarczanego oprogramowania bazodanowego. 2) Przeniesienie konfiguracji aktualnie działającego środowiska HIS, LIS Eskulap na nową wersję bazy danych. 3) Przeprowadzenie testów działania na podstawie kopi zapasowej udostępnionej przez Zamawiającego wraz z wykonaniem dokumentacji powykonawczej. Powyższe usługi muszą zostać wykonane w sposób zapewniający po ich realizacji bezawaryjną prace eksploatowanych przez Zamawiającego systemów. 4) Przeniesienie i tuning bazy danych w oparciu o dostarczany motor bazy danych do nowego środowiska. Całe rozwiązanie musi być zgodnie z polityką licencjonowanie producenta bazy danych. Zamawiający wymaga aby tuning bazy danych wykonywany był raz do roku w ramach 3 gwarancji. 5) Testy weryfikacyjne powinny obejmować przynajmniej: • zestawienie poprawnego podłączenia systemu HIS,LIS,RIS,PACS systemu Eskulap, • podłączenie z aparatami, sterownikami do systemu HIS, • poprawność generowania sprawozdań, • weryfikacja połączenia z usługami dodatkowymi (EWUŚ, gruper JGP itp.).

2. Serwer backupowy

Lp.	Obszar	Wymaganie
1.	Obudowa	1.1. Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia). 1.2. Zainstalowany moduł TPM 2.0
2.	Procesory	2.1. 2 procesory o parametrach opisanych poniżej. 2.2. Procesor 8 rdzeniowy, x86 - 64 bity, minimalne taktowanie bazowe (bez trybu Turbo) ma wynosić 2,1GHz. Procesor osiągający w testach CPUbenchmark Multiple CPU Systems dostępnych na stronie https://www.cpubenchmark.net/multi_cpu.html wynik minimum 18500 punktów.
3.	Pamięć operacyjna	3.1. Zainstalowane 256 GB pamięci RAM typu DDR4 Registered, 2933Mhz w kościach o pojemności 32 GB. 3.2. Obsługa zabezpieczeń: Advanced ECC lub Adaptive double device data correction (ADDDC), Failed DIMM isolation, MemoryMirror 3.3. Serwer musi obsługiwać pamięci typu NVDIMM. 3.4. Serwer musi posiadać minimum 24 gniazda pamięci RAM na płycie głównej, obsługa minimum 2 TB pamięci RAM DDR4 2933 Mhz.

4.	Sloty rozszerzeń	4.1. Serwer musi posiadać minimum 6 aktywnych gniazd PCI-Express min. generacji 3 o prędkości min. x8 i jedno o prędkości x16 , gotowych do obsadzenia kartami rozszerzeń .
5.	Dyski twarde	5.1. Zainstalowane 2 dyski min. 480GB M.2 SSD zabezpieczone RAID 1 poprzez dedykowany kontroler RAID, dyski HotSwap. 5.2. Zainstalowane 12 dysków min. 4TB Nl-SAS 7,2k 3,5” Hot Swap.
6.	Kontroler	6.1. Serwer musi być wyposażony w kontroler sprzętowy z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę min. 8 napędów dyskowych.
7.	Interfejsy sieciowe Ethernet i FC	7.1. Minimum 4 porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCI-E opisanych pkt 4. 7.2. Minimum 2 dwuportowe karty 10Gb Eth Base-T. 7.3. Wszystkie porty ethernet muszą wspierać protokół LACP. 7.4. Karty ethernet muszą umożliwiać podział na wirtualne interfejsy. 7.5. Minimum 2 porty FC, każdy port 16 Gb/s. Wszystkie porty wraz z wkładkami SFP+ 16 Gb SW.
8.	Porty	8.1. 2 porty USB 3.0. 8.2. 1 port VGA 8.3. 1 port Serial 8.4. 1 port Zarządzania serwerem 8.5. Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera.
9.	Zasilacze	9.1. Min. 2 redundantne zasilacze (1+1), typu HotPlug o mocy minimum 550W każdy.
10.	Karta/moduł zarządzający	Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: 10.1. Niezależny od systemu operacyjnego, umożliwiający pełne zarządzanie, zdalny restart serwera; 10.2. Dostęp przez kartę LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; 10.3. Dostęp poprzez przeglądarkę Web (także SSL, SSH) 10.4. Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii 10.5. Zarządzanie alarmami (zdarzenia poprzez SNMP) 10.6. Możliwość przejęcia konsoli tekstowej 10.7. Opcjonalne przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) 10.8. Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych) 10.9. Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.). Serwer musi mieć możliwość zarządzania przez dedykowana aplikację mobilną na systemy IOS oraz Android, wyprodukowaną przez producenta serwera, darmową oraz umożliwiającą z poziomu tej aplikacji co najmniej: - wyświetlenie informacji o stanie serwera, modelu, adresie IP karty zarządzającej, wersji BIOS, wersji oprogramowania zarządzającego, zainstalowanych procesorach, zainstalowanej pamięci RAM, zainstalowanym kontrolerze RAID - sprawdzenia temperatury serwera oraz podzespołów, w tym co najmniej CPU oraz RAM -sprawdzenie aktualnego poboru mocy przez serwer

		- włączenie oraz wyłączenie serwera -uruchomienia diod na froncie obudowy w celu wizualnej identyfikacji serwera w szafie rack - zmianę adresu IP karty zarządzającej
11.	Dodatkowe funkcje	11.1 Zainstalowany system operacyjny Windows Server 2019 Standard z Software Assurance lub równoważny*. Licencja musi obsłużyć serwer fizyczny wyposażony w 1 procesory oraz 16 rdzeni. Licencja z prawem do aktualizacji do następnej wersji systemu operacyjnego.
12.	Wsparcie techniczne	12.1 3-letnia gwarancja producenta w miejscu instalacji. 12.2 Zgłoszenia przyjmowane w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta lub autoryzowany przez producenta serwis. 12.3 Czasy reakcji i naprawy: - czas reakcji w formule NBD - czas naprawy awarii zgodnie ze standardowymi warunkami producenta, jednak czas ten nie może być dłuższy niż 5 dni. - czas gwarancji – zgodnie z OPZ 10.1. W przypadku uszkodzenia nośnika danych (dysku), uszkodzony nośnik pozostaje u Zamawiającego.
	Inne	- Sprzęt musi pochodzić z autoryzowanego przez jej producenta kanału dystrybucji w UE i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim. - Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych - Wszystkie urządzenia muszą być fabrycznie nowe. Przed dostawą sprzęt musi być zarejestrowany przez producenta, bezpośrednio na Zamawiającego jako jedynego użytkownika po opuszczeniu fabryki. - Zamawiający może zażądać przed dostawą dokumentu zawierającego listę numerów seryjnych dostarczanego sprzętu w celu weryfikacji spełnienia warunków gwarancyjnych. Zamawiający sprawdzi spełnienie powyższych warunków w polskim biurze producenta na podstawie numeru seryjnego urządzenia – w przypadku niezgodności deklaracji Wykonawcy z opinią producenta - Zamawiający odmówi odbioru przedmiotu zamówienia, jako niezgodnego ze specyfikacją istotnych warunków zamówienia.
13.	Usługi	Usługa montażu, integracji i konfiguracji funkcji serwera w miejscu wskazanym przez zamawiającego zgodnie z jego specyfikacją. Dokładny zakres wdrożenia zostanie ustalony na etapie realizacji z zamawiającym i będzie składał się z dowolnych wymagań zawartych w OPZ.

3. Przełącznik dystrybucyjny

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
Przełącznik dystrybucyjny– specyfikacja przedmiotu zamówienia		
1.	Obudowa	Przełącznik musi posiadać obudowę wolnostojącą, umożliwiająca montaż w 19-calowym stelażu telekomunikacyjnym (standard EIA) lub w specjalnej szafce na sprzęt (akcesoria montażowe w komplecie). Przełącznik wyposażony w co najmniej jeden wymienny zasilacz 230V/AC

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
2.	Ilość portów	Min 48 portów RJ-45 auto-negotiating 10/100/1000 PoE+ (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T, IEEE 802.3af PoE, IEEE 802.3at), budżet mocy dla funkcji PoE minimum 370 W Min 4 porty 1/10GE SFP/SFP+,
3.	Dodatkowe porty	Min 1 port RJ45 do zarządzania poprzez konsolę, Min 1 wbudowany, dodatkowy, dedykowany port Ethernet do zarządzania poza pasmem - out of band management
4.	Zarządzanie	Musi priorytetyzować pakiety na podstawie DSCP lub IEEE 802.1p (np. Dla VoIP i VIDEO) Musi zarządzać przepustowością danej transmisji Musi obsługiwać Class of Service (CoS)
5.	Zarządzanie jakością (QoS)	Musi priorytetyzować pakiety na podstawie DSCP lub IEEE 802.1p (np. Dla VoIP i VIDEO) Musi zarządzać przepustowością danej transmisji Musi obsługiwać Class of Service (CoS)
6.	Warstwa przełączania	Przepustowość Min. 130 Mpps Prędkość przełączenia Min. 170Gbps Wielkość tablicy MAC: Min. 16384 Ilość obsługiwanych jednocześnie, aktywnych Vlanów: min. 4094 Auto MDIX/ Musi obsługiwać automatyczne dostosowanie prędkości i typu połączenia na portach 10/100/1000 Tablica ARP: minimum 4000 wpisów Tablica routingu: nie mniejsza niż 4000 wpisów dla IPv4 i 1000 wpisów dla IPv6 Agregacja portów: zgodna z 802.3ad LACP Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie
7.	Pamięć	Co najmniej 1GB SDRAM, min. 128MB flash;
8.	Funkcje wysokiej dostępności	Musi obsługiwać następujące protokoły: - Spanning Tree (802.1d), - Rapid Convergence Spanning Tree (802.1w), - Muliple Spanning Trees (802.1s) - Wsparcie dla protokołu typu Ethernet Ring Protection Switching (ERPS, G.8032 v1 i v2)
9.	Bezpieczeństwo	W ramach bezpieczeństwa musi obsługiwać: - SSL, - https, - ACL - STP BPDU port protection - STP root guard - logowanie po IEEE 802.1X i RADIUS - DoS (Automatic) - Management password - Automatic VLAN Assignment - Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego
10.	Monitorowanie	Musi obsługiwać: - denial-of-service protection - Port mirroring - RMON

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
11.	Pozostałe funkcje	Przełącznik musi dodatkowo obsługiwać: - Network Time Protocol (NTP) - Energy Efficient Ethernet - Management password - LLDP-MED - LLDP - IGMP/MLD snooping - Auto Voice VLAN - wsparcie dla FTP, - możliwość stackowania do 9 urządzeń w stosie - Packet storm protection
12.	Oprogramowanie	Urządzenie musi mieć zapewnione bezpłatne aktualizacje przez cały okres posiadania sprzętu - dostępne na stronie producenta
13.	Informacje dodatkowe	- Sprzęt musi pochodzić z autoryzowanego przez jej producenta kanału dystrybucji w UE i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim. - Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych - Wszystkie urządzenia muszą być fabrycznie nowe. Przed dostawą sprzęt musi być zarejestrowany przez producenta, bezpośrednio na Zamawiającego jako jedynego użytkownika po opuszczeniu fabryki. - Zamawiający może zażądać przed dostawą dokumentu zawierającego listę numerów seryjnych dostarczanego sprzętu w celu weryfikacji spełnienia warunków gwarancyjnych. Zamawiający sprawdzi spełnienie powyższych warunków w polskim biurze producenta na podstawie numeru seryjnego urządzenia – w przypadku niezgodności deklaracji Wykonawcy z opinią producenta - Zamawiający odmówi odbioru przedmiotu zamówienia, jako niezgodnego ze specyfikacją istotnych warunków zamówienia.
14.	Gwarancja	3 letnia gwarancja producenta. Gwarantowany czas naprawy sprzętu maksymalnie 5 dni od momentu zgłoszenia. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia.
15.	Usługi	Usługa montażu, integracji i konfiguracji funkcji przełączników w miejscu wskazanym przez zamawiającego, zgodnie z ich specyfikacją. Dokładny zakres wdrożenia zostanie ustalony na etapie realizacji z zamawiającym i będzie składał się z dowolnych wymagań zawartych w OPZ.

4. Moduły SPF+ typ 1

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
Moduły SFP+ dla przełączników dystrybucyjnych – wym. w pkt.3 Przełącznik dystrybucyjny		
1.	Typ interfejsu	SFP+
2.	Maksymalna szybkość przesyłania danych	10000 Mbit/s
3.	Złącze światłowodowe	LC

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
4.	Maksymalny dystans transferu	300 m
5.	Typ transceivera SFP	Fiber optic; typ Multi Mode
6.	Inne	W pełni kompatybilne z zakupywanymi przełącznikami dystrybucyjnymi
7.	Gwarancja	1) czas naprawy awarii, zgodnie ze standardowymi warunkami producenta, jednak czas ten nie może być dłuższy niż 5 dni. 2) czas trwania gwarancji – zgodnie z OPZ.

5. Moduły SPF+ typ 2

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
Moduły SFP+ dla przełączników dystrybucyjnych – wym. w pkt.3 Przełącznik dystrybucyjny		
1.	Typ interfejsu	SFP+
2.	Maksymalna szybkość przesyłania danych	10000 Mbit/s
3.	Złącze światłowodowe	LC
4.	Maksymalny dystans transferu	2000 m
5.	Typ transceivera SFP	Fiber optic; typ Single Mode
6.	Inne	W pełni kompatybilne z zakupywanymi przełącznikami dystrybucyjnymi
7.	Gwarancja	1) czas naprawy awarii, zgodnie ze standardowymi warunkami producenta, jednak czas ten nie może być dłuższy niż 5 dni. 2) czas trwania gwarancji - zgodnie z OPZ.

6. Napęd taśmowy z taśmami

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
Napęd taśmowy z taśmami– specyfikacja przedmiotu zamówienia		
1	Obudowa	Obudowa przeznaczona do montażu w szafie przemysłowej 19”. Biblioteka o wysokości maksymalnej 3U. Należy dostarczyć niezbędne elementy potrzebne do montażu biblioteki w szafie
2	Obsługiwane napędy	Obsługa napędów LTO-6, LTO-7 oraz LTO-8 z interfejsem FC
3	Zainstalowane napędy	Jeden napęd taśmowy klasy LTO 7 z interfejsem FC 8Gb
4	Sposób pracy napędu	Napęd taśmowy musi być wyposażony w mechanizm dostosowujący automatycznie oraz płynnie prędkość przesuwu taśmy magnetycznej do wartości strumienia danych przekazywanego do napędu w zakresie co najmniej 101-300MB/s.
5	Zabezpieczenie danych	Obsługa sprzętowego szyfrowania danych w standardzie AES 256-bit dla wszystkich obsługiwanych typów napędów taśmowych.
6	Liczba slotów na kasety	Oferowana biblioteka musi być wyposażona w co najmniej 25 slotów na taśmy magnetyczne.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
7	Sposób obsługi wymiany taśm w bibliotece	Oferowana biblioteka taśmowa musi posiadać możliwość konfiguracji tzw. „mail slot" umożliwiającego wymianę taśm bez konieczności wyjmowania z biblioteki całego magazynka z taśmami. Musi umożliwiać skonfigurowanie przynajmniej 15 slotów Import/Export
8	Dodatkowe funkcjonalności	Możliwość stosowania taśm typu WORM. Mechanizm automatycznego czyszczenia głowic, brak konieczności cyklicznej obsługi konserwacyjnej przez personel techniczny. Oferowana biblioteka musi być wyposażona w czytnik kodów kreskowych. Wsparcie dla następującego oprogramowania służącego do tworzenia kopii bezpieczeństwa - Veritas NetBackup - Veritas Backup Exec - CommVault - arcserve Arcserve Backup - Veeam Software Biblioteka musi oferować budowę modułową i umożliwiać: -minimalna ilość slotów po rozbudowie - 400 -minimalna ilość napędów po rozbudowie - 24 Biblioteka musi mieć możliwość utworzenia do 12 partycji
9	Taśmy	25 taśmy LTO-7 RW z nalepkami z kodami kreskowymi. 1 taśma czyszcząca
10	Oprogramowanie zarządzające	Oferowana biblioteka taśmowa musi posiadać możliwość zdalnego zarządzania za pośrednictwem przeglądarki internetowej. Oferowana biblioteka musi być wyposażona w oprogramowanie umożliwiające aktywne monitorowanie. Wsparcie dla protokołu SNMP. Jeśli powyższe funkcjonalności wymagają dodatkowych licencji, należy je dostarczyć wraz z urządzeniem.
11	Okablowanie	Do urządzenia należy dołączyć okablowanie zasilające i służące do transmisji danych (FC, Eth)
12	Niezawodność	Parametr MSBF (mean swaps between failures) o wartości 2 000 000 dla pełnych cykli „załaduj/wyładuj". Parametr MTTR nie większy niż 30 minut Biblioteka musi mieć możliwość stworzenia do 12 bibliotek ,,logicznych" Biblioteka musi być wyposażona w nadmiarowe zasilacze
13	Gwarancja	Serwis powinien być realizowany przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta w zakresie serwisu gwarancyjnego przez okres 36 miesięcy. Oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Polski), mających swoją siedzibę na terenie Polski. Podmiot realizujący serwis powinien posiadać ISO 9001 w zakresie świadczenia usług serwisowych Zgłoszenia serwisowe przyjmowane w trybie 9x5 z czasem reakcji 1 godzina, przez dedykowany serwisowy moduł internetowy (należy podać adres www) oraz infolinię dostępną w trybie 8x5 (należy podać numer infolinii) z czasem reakcji 1 godziny. Komunikacja telefoniczna i elektroniczna powinna być realizowana w języku polskim. Serwis powinien zapewnić rozpoczęcie procedury naprawy przez certyfikowanego serwisanta najpóźniej w następnym dniu roboczym od zgłoszenia.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		Oferent winien przedłożyć dokumenty: -Oświadczanie Producenta lub Autoryzowanego Partnera Serwisowego świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). -Certyfikat ISO 9001 podmiotu serwisującego.
14	Inne	- Sprzęt musi pochodzić z autoryzowanego przez jej producenta kanału dystrybucji w UE i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim. - Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych - Wszystkie urządzenia muszą być fabrycznie nowe. Przed dostawą sprzęt musi być zarejestrowany przez producenta, bezpośrednio na Zamawiającego jako jedynego użytkownika po opuszczeniu fabryki. - Zamawiający może zażądać przed dostawą dokumentu zawierającego listę numerów seryjnych dostarczanego sprzętu w celu weryfikacji spełnienia warunków gwarancyjnych. Zamawiający sprawdzi spełnienie powyższych warunków w polskim biurze producenta na podstawie numeru seryjnego urządzenia – w przypadku niezgodności deklaracji Wykonawcy z opinią producenta - Zamawiający odmówi odbioru przedmiotu zamówienia, jako niezgodnego ze specyfikacją istotnych warunków zamówienia.
15	Usługi	Usługa montażu, integracji i konfiguracji funkcji biblioteki w miejscu wskazanym przez zamawiającego zgodnie z jej specyfikacją. Dokładny zakres wdrożenia zostanie ustalony na etapie realizacji z zamawiającym i będzie składał się z dowolnych wymagań zawartych w OPZ.

7. Punkt dostępowy Wifi

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
Punkt dostępowy Wifi– specyfikacja przedmiotu zamówienia		
1.	Prędkość /transfer danych przez Ethernet LAN	10,100,1000 Mbit/s
2.	Maksymalny transfer danych przez bezprzewodowy LAN	1100 Mbit/s
3.	Maksymalna szybkość przesyłania danych	1000 Mbit/s
4.	Maksymalny zakres wewnętrzny (pomieszczenie)	Min 100 m

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
5.	Przycisk reset	Tak
6.	Certyfikaty	CE, FCC, IC
9.	Poziom wzmocnienia anteny (max)	Każdy z modułów radiowych musi posiadać trzy wewnętrzne, zintegrowane, dookólne anteny o zysku energetycznym a) 21 dBm dla 2.4 GHz, b) 21 dBm dla 5 GHz
10.	Ilość anten	2
11.	Zasilanie	Wymagane jest, aby zasilanie urządzenia było zrealizowane za pośrednictwem 802.3af PoE lub 802.3at PoE+
12.	Szyfrowanie transmisji bezprzewodowych	WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3, TKIP/AES)
13.	Pasmo pracy	2,4GHz oraz 5GHz
14.	Architektura	Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera: a. Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https b. Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki c. Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania. Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2: a. System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako elementu zarządzającego b. W przypadku awarii punktu zarządzającego kolejny punkt dostępowy w sieci musi przejąć jego rolę w sposób automatyczny c. Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe d. Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję e. Tworzenie klastra do 140 urządzeń
15.	Zarządzanie transmisją	802.1Q, QoS, tryb Hotspot, portal dla gości, Izolacja ruchu gości, MultiSSID (minimum 16 jednocześnie na każdym module radiowym)

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
16.	Inne	Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP Punkt dostępowy musi mieć możliwość pracy jako analizator widma W system operacyjny musi być wbudowana pełnostanowa zapora sieciowa Sprzęt musi pochodzić z autoryzowanego przez jej producenta kanału dystrybucji w UE i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim. Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych Wszystkie urządzenia muszą być fabrycznie nowe. Przed dostawą sprzęt musi być zarejestrowany przez producenta, bezpośrednio na Zamawiającego jako jedynego użytkownika po opuszczeniu fabryki. Zamawiający może zażądać przed dostawą dokumentu zawierającego listę numerów seryjnych dostarczanego sprzętu w celu weryfikacji spełnienia warunków gwarancyjnych. Zamawiający sprawdzi spełnienie powyższych warunków w polskim biurze producenta na podstawie numeru seryjnego urządzenia – w przypadku niezgodności deklaracji Wykonawcy z opinią producenta - Zamawiający odmówi odbioru przedmiotu zamówienia, jako niezgodnego ze specyfikacją istotnych warunków zamówienia.
17.	Zestaw montażowy	Punkt dostępowy zostanie dostarczony z uchwytem umożliwiającym instalację naścienną/sufitową.
18.	Gwarancja	1) czas naprawy awarii, zgodnie ze standardowymi warunkami producenta, jednak czas ten nie może być dłuższy niż 5 dni. 2) czas trwania gwarancji - zgodnie z OPZ.
19.	Usługi	Usługa montażu, integracji i konfiguracji funkcji punktów dostępowych i kontrolera w miejscu wskazanym przez zamawiającego, zgodnie z ich specyfikacją. Dokładny zakres wdrożenia zostanie ustalony na etapie realizacji z zamawiającym i będzie składał się z dowolnych wymagań zawartych w OPZ.

8. UTM

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
UTM– specyfikacja przedmiotu zamówienia		
		Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. System bezpieczeństwa UTM musi zostać dostarczony w klastrze wysokiej dostępności co najmniej Active-Passive. Dla dostarczonych elementów systemów bezpieczeństwa wykonawca musi zapewnić wszystkie poniższe funkcjonalności: 1) Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent. 2) System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. Dopuszcza się system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej z

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		wykluczeniem platform sprzętowych lub programowych, które wysyłają logi do chmury zlokalizowanej poza terenem Unii Europejskiej. 3) W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności: a) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection b) Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS). System AV musi umożliwiać skanowanie AV dla co najmniej plików typu: rar, zip. c) Poufność danych - IPSec VPN oraz SSL VPN d) Ochrona przed atakami - Intrusion Prevention System (IPS/IDS) e) Kontrola stron Internetowych – Web Filter f) Kontrola poczty – antyspam (dla protokołów SMTP, POP3) g) Kontrola pasma oraz ruchu (QoS i Traffic shaping) h) Kontrola aplikacji oraz rozpoznawanie ruchu P2P i) Analiza ruchu szyfrowanego protokołem SSL 4) W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż: a) Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site b) Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem c) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności d) Praca w topologii Hub and Spoke oraz Mesh e) Obsługa mechanizmów: IPSec f) Obsługa ssl vpn w trybach portal oraz tunel 5) Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP. 6) Translacja adresów NAT adresu źródłowego i NAT adresu docelowego. 7) Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety). 8) Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 9) Sygnatury AV muszą być weryfikowane i udostępniane na serwerach producenta systemu bezpieczeństwa. 10) Oferowany system bezpieczeństwa nie może wysyłać plików poza teren Unii Europejskiej, pliki nie mogą być też udostępniane innym podmiotom. 11) Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać co najmniej 1500 wpisów. Dodatkowo musi być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS. 12) Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 13) Baza filtra WWW. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW. 14) Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL. 15) System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników w oparciu o zewnętrzną bazę RADIUS lub Active Directory

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		16) W zakresie realizowanych funkcjonalności systemu raportowania i przeglądania logów, wymagane jest nie mniej niż: a) Posiadanie predefiniowanych raportów dla ruchu WWW, modułu IPS, skanera antywirusowego i antyspamowego. 17) System raportowania i przeglądania logów wbudowany w system bezpieczeństwa nie może wymagać dodatkowej licencji do swojego działania. 18) Oferowany system bezpieczeństwa po zakończeniu trwania licencji nie może zablokować pracujących na nim modułów bezpieczeństwa. System będzie pracował na sygnaturach i regułach pobranych w ostatnim dniu aktywnej licencji. 19) Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 20) Interfejsy 2 x 10GE (SFP+) + 8 x GE Combo 21) Pamięć wewnętrzna 240 GB 22) Przepustowość IPSec min 6 Gbps 23) Maks. liczba tuneli IPSec min 4 000 24) Maks. liczba tuneli SSL min 100 25) Liczba jednoczesnych sesji 4 000 000 26) Nowe sesje / sekundę 80 000 27) 802.1Q VLAN (max) 256 28) Firewall 9 Gbps (1518-byte, UDP) 29) Firewalle muszą zostać dostarczone z 3 letnią licencją na funkcjonalności IPS/AV/URL Filtering w ramach której urządzenie może automatycznie aktualizować bazy sygnatur ze strony producenta.
	Gwarancja	3 letnia gwarancja. Gwarantowany czas naprawy sprzętu – 48h od momentu zgłoszenia. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia.
	Inne	Sprzęt musi pochodzić z autoryzowanego przez jej producenta kanału dystrybucji w UE i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim. Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych Wszystkie urządzenia muszą być fabrycznie nowe. Przed dostawą sprzęt musi być zarejestrowany przez producenta, bezpośrednio na Zamawiającego jako jedynego użytkownika po opuszczeniu fabryki. Zamawiający może zażądać przed dostawą dokumentu zawierającego listę numerów seryjnych dostarczanego sprzętu w celu weryfikacji spełnienia warunków gwarancyjnych. Zamawiający sprawdzi spełnienie powyższych warunków w polskim biurze producenta na podstawie numeru seryjnego urządzenia – w przypadku niezgodności deklaracji Wykonawcy z opinią producenta Zamawiający odmówi odbioru przedmiotu zamówienia, jako niezgodnego ze specyfikacją istotnych warunków zamówienia.
	Usługi	Usługa montażu, integracji i konfiguracji funkcji UTM w miejscu wskazanym przez zamawiającego zgodnie z ich specyfikacją. Dokładny zakres wdrożenia zostanie ustalony na etapie realizacji z zamawiającym i będzie składał się z dowolnych wymagań zawartych w OPZ.

9. Szafa serwerowa

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
Szafa serwerowa– specyfikacja przedmiotu zamówienia		
1.	Wymagania ogólne	Dostarczyć należy wyposażoną szafę typu Rack 47U (przeznaczoną do instalacji i eksploatacji sprzętu IT). Wewnątrz szafy zainstalowana musi być jednostka klimatyzacji w oparciu o instalację DX – bezpośrednie odparowanie z zewnętrznym skraplaczem. W celu zapewnienia najwyższego stopnia wymaganej bezawaryjności, dostępności, wydajności i efektywności energetycznej, skalowalności całości budowanego układu oraz najwyższego stopnia bezpieczeństwa pracy powinny zostać zastosowane wszystkie wymienione niżej urządzenia produkowane przez jednego producenta: a) urządzenia chłodnicze, parowniki, zintegrowane w szafie 19” w układzie zamkniętym, chłodzenie w sposób neutralny dla temp. powietrza w pomieszczeniu, b) skraplacze zewnętrzne, c) szafy 19” IT, d) urządzenia gaśnicze wraz z wczesną detekcją pożaru, e) system zdalnego monitoringu warunków środowiskowych.
2.	Urządzenia chłodnicze zintegrowane w szafie 19” IT	1. Klimatyzator typu split DX o mocy 6,5 kW składający się z jednostki wewnętrznej (parownik) i jednej jednostki zewnętrznej (chłodziarki z regulacją inwerterową). 2. Konstrukcja jednostki wewnętrznej umożliwiająca zainstalowanie w szafie IT o szerokości 800 mm, montowana wewnątrz szafy IT pomiędzy ramą 19” a ścianą boczną szafy IT. Konstrukcja zoptymalizowana pod kątem IT w taki sposób, aby idealnie wspomagać prowadzenie powietrza „Front to Back“ zabudowy 19". Jednostka wewnętrzna zasysająca ciepłe powietrze wylotowe z serwerów bezpośrednio w tylnej części szafy a schłodzone wydmuchiwane po bokach przed płaszczyzną 19". Obudowa jednostki wewnętrznej wykonana z blachy stalowej powlekanej proszkowo, wewnątrz parownik bezpośredni, 4 wentylatory promieniowe EC, kolektor i odpływ kondensatu. 3. Urządzenia powinno pozwalać na montaż z lewej lub z prawej strony szafy serwerowej IT. Jednostka wewnętrzna powinna być wyposażona w sterownik mikroprocesorowy do regulacji temperatury powietrza na wlocie do serwera. Zakres nastawy temperatury wlotowej na serwer to przedział od 20°C do 28°C. 4. Wchodzący w skład systemu zewnętrzny czujnik powinien być umieszczony przed serwerem. Jednostka zewnętrzna ze sprężarką powinna posiadać regulację inwerterową umożliwiającą bezstopniowe dopasowanie mocy także podczas pracy w trybie obciążenia częściowego. Połączenie między jednostką wewnętrzną a zewnętrzną powinno odbywać się za pomocą rurek miedzianych, przewodu danych i zasilania elektrycznego. Urządzenie wewnętrzne zasilane przez napięcie z urządzenia zewnętrznego. 5. Jako czynnik chłodniczy powinien zostać zastosowany R410a.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		Dane techniczne: 1. Użytkowa moc chłodnicza maksymalnie 6,5 kW 2. Zainstalowane wentylatory w jednostce wewnętrznej: 4 3. Podstawa regulacji: temperatura powietrza na wlocie do serwera, ustawiona na maksimum 22°C 4. Zasilanie elektryczne: 230V, 1~, N, PE, 50 Hz 5. Zabezpieczenie: 16A 6. Czynnik chłodniczy: R410a 7. Wymiary jednostki wewnętrznej, szer. x wys. x gł.: 105x1550x820 mm 8. Wymiary jednostki zewnętrznej, szer. x wys. x gł.: 845 x 700 x 320 mm 9. Dopuszczalne są różnice w wymiarach +/- 5mm 10. Masa jednostki wewnętrznej: maksymalnie 48 kg 11. Masa jednostki zewnętrznej: maksymalnie 42 kg 12. Zakres temperatur otoczenia, jedn. zewn.: -20°C do +45°C
3.	Szafa 19” serwerowa	1. Integralną częścią systemu chłodzenia w technologii chłodzenia wymiennikiem chłodniczym Rackowym musi być szafa IT - 19”. Wymagane są szafy IT tego samego producenta co wymienników chłodniczych oraz skraplaczy tak, aby zapewniona została jak najwyższa dostępność, spójność rozwiązań i optymalizacja poprawnego działania elementów w całości dostarczonego systemu. 2. Należy dostarczyć szafę 19” IT o wymiarze 800mmx2200mmx1200mm (szerokość x wysokość x głębokość) każda. 3. Minimalne wymagania techniczne, funkcjonalne, wyposażenia dla szaf serwerowych, sieciowych: a) Szafa IT dopuszczona przez producenta do klimatyzacji oraz wczesnego wykrywania i gaszenia pożaru tylko wewnątrz, dla układu zamkniętego, neutralny dla powietrza otoczenia serwerowni. b) Szafa serwerowa, 19”, konstrukcja ramy szaf sztywna, spawana. c) Wysokość zabudowy szaf serwerowych 47U, wraz z dodatkową separacją frontową strefy zimnej. d) Przednie drzwi przeszklone o szczelności IP55 (szkło bezpieczne hartowane ESG 3mm), tylne drzwi dzielone pionowo z blachy stalowej pełne. Płyta dachu pełna. e) Dwie płaszczyzny mocowania 482,6 mm (19“) z przodu i z tyłu na wspornikach montowanych po głębokości szafy w części dachowej oraz podłogowej ramy szafy. f) Łączna obciążalność obu płaszczyzn montażowych 19” min. 1500 kg. Obciążalność szafy potwierdzona odpowiednim dokumentem. g) Płaszczyzny montażowe 19” powinny składać się z uniwersalnych szyn profilowych do zastosowań serwerowych, sieciowych i elektronicznych, z bezstopniową regulacją głębokości, mocowanie do poprzeczek. Mocowanie szyn profilowych powinno odbywać się elastycznie, bez użycia narzędzi, za pomocą szybkozłączy. Szyny profilowe z przodu i z tyłu z dodatkowym otworowaniem w standardzie EIA 310 E. Wszystkie jednostki wysokości powinny być oznakowane na szynach profilowych i ponumerowane w przeciwnych kierunkach. Oznakowanie U obu płaszczyzn montażowych powinno być czytelne od przodu. Wszystkie poprzeczki ze zintegrowaną podziałką do szybkiego określania odstępów montażowych i pozostałej wolnej przestrzeni z przodu. h) Szyny profilowe 19” z przodu muszą być przygotowane do beznarzędziowego montażu elementów ułatwiających prowadzenie kabli i organizowania struktury okablowania o maksymalnej gęstości upakowania.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		i) Szyny profilowe 19” z tyłu muszą być przygotowane do obustronnego zamocowania Power Distribution Unit (PDU) o wymiarze 1U do zelektryfikowania szafy bez zużywania objętości pod zabudowę dzięki montażowi pomiędzy płaszczyzną montażową a ścianą boczną, w przestrzeni zero-U. Montaż PDU możliwy pod dwie PDU na każdą ze stron. j) Szafa o szer. 800mm powinna mieć możliwość realizacji zabudowy 19" w standardzie jako centralna wypośrodkowana lub jako asymetryczna z możliwością przesuwania do skrajnego dowolnego boku szafy. Możliwość realizacji zabudowy profili pod sprzęt IT w standardzie: 19", 21", 23", 24" bez dodatkowych przeróbek mechanicznych, akcesoriów montażowych. k) Akcesoria montażowe 19“ i kompletny zestaw uziemienia dołączone luzem do zestawu. l) Szafę dodatkowo powinna być wyposażona od frontu szafy z mocowaniem do przedniego profilu 19-calowego w częściową pionową prowadnicę powietrza zabudowaną po przeciwnej stronie do wewnętrznego wymiennika DX. Prowadnica powinna posiadać panele zaślepiające 3 x1U - 19", dla dodatkowej pow. montażowej. m) Materiał: - Blacha stalowa, - Tworzywo sztuczne zgodne z UL 94-V0 - Powierzchnia: lakierowana. n) Dla prowadzenia Kabli w pionie szafa musi być dodatkowo wyposażona w koryto montażowe kablowe pionowe, montowane po głębokości szafy na wydzielonym poziomie montażowym. Montaż możliwy bez użycia narzędzi . o) Dla zaślepienia wolnej przestrzeni należy z szafą dostarczyć panele zaślepiające o wysokości min. 9U przeznaczone do beznarzędziowego montażu w 19”. Panele zaślepiające mają zapewnić odpowiednie prowadzenie powietrza oraz zapewnić właściwy sposób rozprowadzenia gazu gaśniczego. Każdy panel musi posiadać: odporność ogniową według UL 94 HB i być samogasnący, możliwość indywidualnego dopasowania wielkości przez wyłamanie wytłaczanych elementów 1U. p) Dodatkowo szafa powinna zostać wyposażona w min. jeden poziomy panel porządkujący 1U wraz z pięcioma wieszakami stalowymi o wym. 43x105mm każdy. Szerokość: 482,6 mm (19"). q) Materiał: - Panel: blacha stalowa, - Wieszak: stal ocynkowana. r) Szafa dostarczona musi zostać wraz z dwoma zintegrowanymi listwami zasilania PDU Metered, opomiarowane na każdą z faz z podłączeniem do sieci zdalnego monitorowania. Przewidziane powinny być dwa tory prądowe dla szafy. Listwy PDU muszą posiadać możliwość montażu w sposób beznarzędziowy w przestrzeni pomiędzy ścianą boczną a profilem 19” z dwoma bliźniaczymi listwami. Dla szafy powinna zostać zastosowana listwa PDU o max. prądzie 1x 32A.
4.	Opis technologiczny PDU w wersji Metered	1. Zakres napięcia wejściowego (L-N):90V – 260(400)V AC, 50-60Hz 2. Prąd wejściowy: 32A 3. Liczba faz: 1 4. Liczba gniazdek typu EN60320/C13 (łącznie): min. 24 5. Liczba gniazdek typu EN60320/C13 (na fazę / bezpiecznik): min. 12 6. Liczba gniazdek typu EN60320/C19 (łącznie): min 4 7. Liczba gniazdek typu EN60320/C19 (na fazę / bezpiecznik): min. 2

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		8. Liczba wyłączników ochronnych: min. 2 9. Liczba elektromagnetycznych wyłączników ochronnych: min. 16A Typ C 10. Wtyk przyłączeniowy wejścia PDU: EN60309 / CEE 11. Długość kabla przyłączeniowego: min. 3m 12. Typ kabla przyłączeniowego: H05-VV 13. Liczba żył: 3 14. Przekrój kabla: 4mm² 15. Szerokość max. obudowy PDU: 44mm (1 U) 16. Głębokość max. obudowy PDU: 70mm 17. Wysokość max. obudowy PDU: 1900mm 18. Materiał PDU: aluminium, anodowane, 19. Adapter mocujący PDU: tworzywo sztuczne, czarny 20. Funkcje pomiaru: Pomiar dla każdej fazy lub zasilania 21. Rejestrowane wartości (na fazę): Napięcie (V), prąd (A), częstotliwość (Hz),Moc czynna (kW), praca czynna (kWh), moc bierna (VA), praca bierna (kVAh), Współczynnik mocy (cos fi), Pomiar przewodu zerowego / określanie obciążenia asymetrycznego, Kontrola wkładki bezpiecznikowej (w wersjach 32A/63A) 22. Zakres pomiaru napięcia: 90V- 260V 23. Rozdzielczość pomiaru napięcia: 0,1V 24. Dokładność pomiaru napięcia: 2% 25. Zakres pomiaru prądu: 0–32A 26. Rozdzielczość pomiaru prądu: 0,1A 27. Dokładność pomiaru prądu: 2% 28. Dokładność pomiaru częstotliwości: 2% 29. Dokładność pomiaru mocy czynnej (kW): 2% 30. Dokładność pomiaru mocy pozornej (KVA): 2% 31. Dokładność pomiaru pracy czynnej (kWh): 1% 32. Dokładność pomiaru pracy biernej (kVAh): 2% 33. Dokładność pomiaru współczynnika mocy: 2% 34. Konfigurowalne wartości graniczne (ostrzeżenie/alarm): Tak 35. Licznik godzin pracy: Tak 36. Wyświetlacz / wskaźniki: OLED, RGB 128x128 pikseli 37. Interfejs sieciowy: RJ45, zintegrowany websewer 38. Obsługiwane protokoły: HTTP, HTTPS, SSL, SSH, NTP, Telnet TCP/IP v4 i v6, DHCP, DNS, NTP, Syslog, SNMP v1, v2c i v3, XMLFTP/SFTP (aktualizacja / transfer plików) Wysyłanie e-maili (SMTP) 39. Administrowanie użytkownikami i uprawnieniami: Tak 40. Integracja z LDAP(S)/Radius/Active Directory: Tak 41. Port USB do aktualizacji firmware i funkcji rejestrowania danych: Tak 42. Interfejs CAN-Bus: RJ45, do podłączania czujników 43. Typy czujników CAN: temperatura, temperatura i wilgotność (kombi), czujnik dostępu IR, czujnik wandalizmu 44. Mini. liczba czujników na 1 PDU: 4 45. Zgodność: CE 46. Bezpieczeństwo: PN-EN 60950-1 47. EMC: PN-EN 55022 / B,PN-EN 61000-4-2,PN-EN 61000-4-3,PN-EN 61000-6-2,PN-EN 61000-6-3 48. Dyrektywa bezpieczeństwa: 2014/35/EU 49. Dyrektywa EMC: 2014/30/EU 50. Stopień ochrony: IP 20 (PN-EN 60529 lub równoważna) 51. Klasa ochrony: Klasa 3 52. Stopień zabrudzenia: 2

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		53. Klasa przepięciowa: II 54. Parametry środowiskowe: RoHS 55. Temperatury otoczenia: 0°C do +45°C 56. Wilgotność otoczenia: 10 - 95% wilg. wzgl., brak kondensacji.
5.	Inne	1. Szafa musi być wyposażona w zintegrowany system wczesnego wykrywania i gaszenia pożaru panelem gaśniczymi o wysokości montażowej max. 1U. 2. Zastosowane urządzenie 1U powinno posiadać wew. zintegrowany pojemnik zawierający środek gaśniczy NOVEC1230 dla kubatury min. 2,8 m3. 3. Gaz przechowywany powinien być w zintegrowanych pojemnikach paneli jako ciecz, która paruje w dyszy gaśniczej i równomiernie rozprasza się w postaci gazu w strefie gaszenia ograniczonego do wnętrza zamkniętych szaf. 4. Środek gaśniczy nie powinien stanowić żadnego ryzyka dla ludzi przebywających w pomieszczeniu, do którego wyzwalany jest środek w stężeniu gaśniczym. 5. Środek gaśniczy wyzwalany powinien być do zamkniętych szaf jako bezbarwny, nieprzewodzący elektryczności i nie korozyjny gaz. Nie wymaga usuwania pozostałości po gaszeniu, nie pozostawia żadnych osadów. Pożar zostaje ugaszony przez odebranie energii cieplnej płomieniom. 6. Detekcja pożaru następowała będzie poprzez dwie czujki pożaru zintegrowane w panelu gaśniczym, powietrze z wnętrza szafy zasysane będzie i analizowane poprzez system dedykowanej instalacji. Informacje o alarmach, awariach, ostrzeżenia, wymaganej konserwacji przesyłane będą do systemu monitorowania warunków środowiskowych. 7. Panel gaśniczy musi posiadać niezależne zintegrowane zasilanie awaryjne na czas min. 4 godz. 8. Szafa 19” musi być wyposażona w czujniki otwarcia drzwi przednich i tylnych monitorujące ich otwarcie oraz rozbrojenie systemu gaszenia na czas otwarcia drzwi.
6	System monitorowania warunków środowiskowych	1. Dla poprawnego działania dostarczonego systemu chłodzenia szafy IT oraz systemu gaszenia musi zostać zastosowany system zdalnego monitorowania warunków fizycznych. 2. System ten powinien być w pełni kompatybilny z funkcjonalnością dostarczonego urządzenia gaśniczego, chłodniczego oraz szafy IT. 3. System musi być oparty o centralną jednostkę sterującą posiadającą jeden adres IP, do której będzie można podłączyć min. 32 czujniki, elementy. 4. Jednostka centralna powinna być podłączona przez Ethernet do sieci danych, konfigurowana przez Web / USB, wysyłać alarmy przez serwer poczty elektronicznej oraz Moduł GSM. 5. Moduł GSM dla komunikacji SMS musi obsługiwać zakresy częstotliwości dla zakresu do 4G włącznie. 6. Dodatkowo powinna istnieć możliwość przesyłania powiadomień alarmowych z mini. 4 innych Modułów zarządzających spiętych w jedna sieć komunikacyjną. 7. Obsługiwane protokoły: TCP/IPv4, TCP/IPv6, SNMPv1, SNMPv2c, SNMPv3, Telnet, SSH, FTP, SFTP, HTTP, HTTPS, NTP, DHCP, DNS, SMTP, Syslog, LDAP, Modbus TCP IP. 8. Zintegrowany WEB serwer 9. Zintegrowany serwer posiadający OPC UA, uniwersalny przemysłowy protokół komunikacyjny umożliwiający komunikację pomiędzy urządzeniami, odczytywanie danych z czujników przez system nadrzędnego sterowania 10. Port szeregowy komunikacyjny RS232

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		11. Możliwość obsługiwania funkcji Server Shutdown, automatycznego zamykania serwerów w zależności od występujących zdarzeń w ramach monitorowanych wybranych parametrów, wymaga określenia na etapie projektu ilości i typu sprzętu IP, klientów, określonych scenariuszy 12. Równoległa do SNMP możliwość komunikacyjna centralnego modułu monitorowania protokołem Modbus TCP IP 13. Stopień ochrony modułów monitoringu: min IP 30 wg PN-EN 60 529 14. Maks. łączna długość przewodów dla magistrali CAN-Bus w jednym module: 100m 15. Obsługa zasilania redundantnego dla modułu centralnego monitoring POE - Power over Ethernet 16. Zegar czasu rzeczywistego z NTP z buforem energii (24h) bez baterii/akumulatora 17. Zarządzanie użytkownikami: LDAP 18. Do zastosowanego systemu zdalnego monitoringu i zarządzania pracą urządzenia gaśniczego, urządzenia chłodniczego, dodatkowo musi zostać zastosowany w szafie 19" IT min. 1 czujnik dualny temperatura-wilgotności, czujnik wycieku punktowy oraz moduł wejścia – wyjścia dla sygnałów bez potencjałowych. 19. Czujnik dualny temperatura-wilgotność. Zakres pomiarowy temp.: 0°C…+55°C, dokładność pomiaru max. +- 1K, rozdzielczość pomiaru zmiany temp. max. 0.1 K. Zakres pomiarowy wilgotności względnej: 1… 99 %, dokładność pomiaru +- 3% w zakresie od 20 do 80% wilgotności względnej. Każdy z zastosowanych czujników temp./ wilgotności musi posiadać: możliwość ustawienia tzw. offsetu czyli korekcji zmierzonych wartości temp. i wilgotności, ustawienia progów wysokiego i niskiego stanu temp. i wilgotności osobno dla stanu ostrzeżenie i alarm, możliwość ustawienia histerezy w mierzonym zakresie temp. i wilgotności. 20. Moduł Wejścia-Wyjścia. Monitorowanie minimalnie ośmiu wejść cyfrowych i sterowanie za pomocą minimalnie czterech wyjść przekaźnikowych. W programie powinna istnieć możliwość połączenia przekaźników i wartości pomiarowych w taki sposób, aby załączały się w określonych okolicznościach. Oprogramowanie musi umożliwiać kontrolę urządzenia lub przekazywać komunikaty. Możliwość szybkiego podłączenia automatycznego rozpoznawania przez plug & play. 21. Zakres temperatury pracy: 0°C…+45°C
7	System automatycznego awaryjnego otwarcia drzwi szafy IT	1. Szafa IT musi zostać wyposażona w zintegrowany system awaryjnego automatycznego otwarcia drzwi przednich i tylnych. 2. Automatyka systemu musi umożliwiać otwarcie drzwi szaf w sposób automatyczny w przypadku braku zasilania oraz awarii układu chłodzenia od ustawionego wzrostu temp. wewnątrz zamkniętej szafy. 3. Szaf musi być wyposażona w system otwarcia drzwi przednich i tylnych: lokalnego manualnego poprzez wkładkę zamka z przyciskiem, zdalnego po sieci oraz automatycznego w przypadku awarii i zadanej logicznej funkcji, scenariusza. W tym celu szafa powinna być wyposażona w odrębny niezależny moduł sterujący otwarciem drzwi szafy wraz z dedykowanym czujnikiem temp. NTC oraz lokalną informacją o granicznych i zadanych temp. wew. szafy. 4. Moduł sterujący zainstalowany w szafie powinien posiadać : 3 wejścia cyfrowe dedykowane dla sygnału alarmu z zewnętrznego systemu/ drzwi przednich / drzwi tylnych, 1 wejście dla czytników zamek cyfrowy / czytnik transponde-

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		rów, 2 wyjścia dla systemu zwolnienia otwarcia drzwi, 2 wyjścia dla opcjonalnego elektrycznego systemu niwelowania podciśnienia w szafie, 2 złącza magistrali przyłączeniowej Can Bus. 5. System powinien być wyposażony w sterownik plug & play dla integracji z opcjonalnym oprogramowaniem DCIM Software. 6. System automatycznego awaryjnego otwarcia drzwi szafy powinien umożliwiać integrację oraz współpracę automatyki z zaprojektowanym wymiennikiem DX. 7. System musi umożliwiać zdalną konfigurację standardowo poprzez Web interfejs oraz opcjonalnie przez oprogramowanie DCIM.
8	Gwarancja	3 letni okres gwarancji ,czas naprawy, zgodnie ze standardowymi warunkami producenta, jednak nie może być dłuższy niż 5 dni. W odniesieniu do czasu trwania gwarancji, obowiązują zapisy OPZ.
9	Usługi	Usługa montażu, instalacji i konfiguracji funkcji szafy w miejscu wskazanym przez zamawiającego, zgodnie z jej specyfikacją. Dokładny zakres wdrożenia zostanie ustalony na etapie realizacji z zamawiającym i będzie składał się z dowolnych wymagań zawartych w OPZ.

10.Licencja dostępowa

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
Licencja dostępowa– specyfikacja przedmiotu zamówienia		
1.	Oprogramowanie	MS Windows 2019 RDS CAL z Software Assurance lub równoważne* - 30 licencji dostępowych na użytkownika.

11.Oprogramowanie backupowe

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
Oprogramowanie backupowe– specyfikacja przedmiotu zamówienia		
1.	Tworzenie Kopii zapasowej	1) Oprogramowanie backupowe obsługujące min. 1 fizyczny serwer bazodanowy oraz min. 2 hosty wirtualizacyjne (zgodne z oprogramowaniem wirtualizacyjnym) Oprogramowanie backupowe ma obsługiwać : a. Jeden host fizyczny - bazę danych Oracle b. Dwa dwa hosty spięte w klaster wirtualizacyjny, które łącznie będą posiadać 2 procesory o łącznej ilości 32 corów." - dopuszcza się rozwiązanie, które wymaga upgrade'u przy rozbudowie środowiska backupowego 2) Obsługiwane systemy operacyjne Windows Serwer 2019, 2016,2012, Linux 3) Obsługiwane platformy minimum VMware i Hyper-V, a także do fizycznych serwerów i stacji roboczych oraz instancji chmurowych 4) Możliwość tworzenia spójnych aplikacyjnie kopii zapasowych maszyn wirtualnych na poziomie obrazu z zaawansowanym przetwarzaniem uwzględniającym specyfikę aplikacji (łącznie z obcinaniem dzienników transakcji). 5) Tworzenie przyrostowych kopii zapasowych poszczególnych maszyn wirtualnych w ramach istniejącego zadania backupu. 6) Udostępnianie macierzystej integracji z obiektową pamięcią masową, obejmującą środowisko lokalne, platformy AWS, Microsoft Azure i IBM Cloud oraz wiele rozwiązań pamięci masowej zgodnych z technologią S3. Pomaga

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		zmniejszyć obciążenia finansowe związane z chmurą publiczną oraz wyeliminować przywiązanie do określonej marki urządzeń dodatkowej pamięci masowej. 7) Możliwość tworzenia dodatkowych migawek pamięci masowej w szerokiej gamie systemów pamięci podstawowej, takich jak HPE 3PAR StoreServ, HPE Nimble oraz NetApp ONTAP i HCI. 8) Pełna kopia syntetyczna 9) Wbudowane funkcje deduplikacji, kompresji i wykluczania plików wymiany 10) Powielanie kopii zapasowych 11) Kompleksowe szyfrowanie 12) Koligacja serwerów proxy 13) Integracja z deduplikującą pamięcią masową 14) Pliki kopii zapasowych poszczególnych maszyn wirtualnych 15) Przetwarzanie na poziomie obrazów z selekcją plików 16) Replikacja maszyn wirtualnych w oparciu o obrazy 17) Wspomagane przełączanie w tryb awaryjny i powrót po awarii 18) Replikacja z kopii zapasowej 19) Planowane przełączanie awaryjne 20) Przełączanie awaryjne jednym kliknięciem 21) Pełne odzyskiwanie maszyny wirtualnej 22) Odzyskiwanie dysków wirtualnych i plików maszyny wirtualnej 23) Portal odzyskiwania plików i maszyn wirtualnych dla operatorów działu wsparcia 24) Portal odzyskiwania elementów programu Microsoft Exchange dla operatorów działu wsparcia 25) Portal odzyskiwania baz danych Microsoft SQL 26) Portal odzyskiwania baz danych Oracle
2.	Usługi	Usługa instalacji, integracji i konfiguracji funkcji systemu backupu zgodnie z jego specyfikacją. Dokładny zakres wdrożenia zostanie ustalony na etapie realizacji z zamawiającym i będzie składał się z dowolnych wymagań zawartych w OPZ.
3.	Gwarancja	Serwis min. 3 lata, z czasem świadczenia usług gwarancyjnych co najmniej 12x5, tj. przez 12 godz. 5 dni roboczych na każdy element oprogramowania.

12. Przełącznik SAN

Lp.	Nazwa komponentu	Wymagania minimalne
1.	Rodzaj przełącznika	Przełącznik musi być wykonany w technologii FC minimum 16 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 8, 16 Gb/s w zależności od rodzaju zastosowanych wkładek SFP+
2.	Wydajność	Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji, gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 16Gb/s. Całkowita przepustowość przełącznika FC musi wynosić minimum 768 Gb/s end-to-end.
3.	Ilość portów	Przełącznik FC musi posiadać minimum 16 portów FC. Wszystkie porty, w które wyposażony jest przełącznik muszą być aktywne. Wszystkie porty muszą być wyposażone we wkładki 16Gb/s SFP+
4.	Rodzaj obsługiwanych portów	Co najmniej: E, F, Diagnostic Port

5.	Kable optyczne	Przełącznik musi zostać dostarczony z kompletem kabli optycznych LC-LC klasy OM4 o długości minimum 15m przeznaczonych dla wszystkich aktywnych portów FC wyposażonych we wkładki SFP+ SW
6.	Typ obudowy	Przełącznik FC musi być przystosowany do montażu w szafie typu rack 19”, o wysokości maksymalnie 1U. Przełącznik musi być wyposażony w akcesoria umożliwiające montaż w szafie
7.	Zasilanie	Przełącznik FC musi posiadać minimum 1 zasilacz.
8.	Agregacja połączeń	Przełącznik FC musi być wyposażony w mechanizm agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu ISL. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC, a połączenie logiczne musi zachowywać kolejność przesyłanych ramek (jeśli funkcjonalność ta wymaga dodatkowej licencji, dostarczenie jej na tym etapie jest wymagane.
9.	Zoning	Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN
10.	Aktualizacja przełącznika	Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware’u (zarówno na wyższą wersję jak i niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC
11.	Bezpieczeństwo	Przełącznik FC musi wspierać mechanizmy zwiększające poziom bezpieczeństwa: • uwierzytelnianie przełączników w sieci fabric za pomocą protokołów DH-CHAP i FCAP; • uwierzytelnianie urządzeń końcowych w sieci fabric za pomocą protokołu DH-CHAP; • szyfrowanie połączenia z konsolą administracyjną (wsparcie dla SSHv2); • definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control); • definiowane kont administratorów w środowisku RADIUS i LDAP w MS Active Directory, Open LDAP, TACACS+; • szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS; • obsługa minimum SNMP v3; • IP Filter dla portu administracyjnego przełącznika; • wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP; • wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP
12.	Sposób zarządzania	Przełącznik FC musi mieć możliwość konfiguracji przez polecenia tekstowe w interfejsie znakowym konsoli terminala oraz przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie. Interfejs graficzny oprogramowanie musi umożliwiać podstawową konfiguracje przełącznika, diagnostykę połączeń, konfiguracje portów, konfiguracje połączeń pomiędzy hostami a macierzami, analiza błędów ramek, wszystkich połączeń FC, które obsługuje przełącznik, tworzenie użytkowników, wykonywanie kopii konfiguracji przełącznika.
13.	Diagnostyka i analiza ruchu FC	Przełącznik FC musi być wyposażony w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC: • logowanie zdarzeń poprzez mechanizm „syslog”,

		• ciągłe monitorowanie parametrów pracy przełącznika, portów, wkładek SFP i sieci fabric z automatycznym powiadamianiem administratora (e-mail) w przypadku przekroczenia zdefiniowanych wartości granicznych (jeśli funkcjonalność ta wymaga dodatkowej licencji, dostarczenie jej na tym etapie jest wymagane) • port diagnostyczny tzw. D_port, który umożliwia wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami, testowe obciążenie połączenia pełną przepustowością 16Gb/s oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością do 5m dla wkładek SFP 16Gb/s (testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric); • FCping; • FCtraceroute; • kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przełącznika
14.	Dostęp	Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, port szeregowy oraz inband IP-over-FC
15.	Wsparcie SMI-S	Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S
16.	Logiczne przełączniki	W przełączniku FC musi istnieć możliwość wydzielenia logicznych, izolowanych od siebie przełączników. Każdy z logicznych przełączników musi mieć własny Domain ID, własne usługi fabric (tzw. fabric services), niezależną bazę zoningu oraz możliwość przypisania dedykowanego administratora.
17.	Kategoryzacja ruchu	Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zoningu.
18.	Mechanizmy QoS	Przełącznik FC musi umożliwiać wprowadzenie ograniczenia prędkości dla danych wchodzących dla dowolnego portu lub portów. Musi być możliwość określenia wartości limitu przepustowości danych wchodzących niższej niż wynegocjowana prędkość portu.
19.	NPIV	Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.
20.	Dodatkowe wymagania	Wszystkie opisane funkcje przełącznika mają być dostępne w urządzeniu na dzień składania ofert i być udokumentowane w publicznie dostępnej dokumentacji na stronach internetowych producenta. Przełącznik musi spełniać wszystkie minimalne wymagania.
21.	Gwarancja	Minimum 36-miesięczna gwarancja świadczona w siedzibie Zamawiającego. Możliwość zgłoszenia awarii przez 24 godziny na dobę. Czas naprawy awarii, nie może być dłuższy niż 5 dni. Czas gwarancji – zgodnie z OPZ. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z przełącznikiem oraz oprogramowania wewnętrznego przełącznika. Serwis musi być realizowany w języku polskim.
22.	Wkładki	Przełącznik musi być w całości wyposażony we wkładki SFP+ min. 16 Gb/s SW FC SFP. Wkładki muszą być kompatybilne z dostarczonym sprzętem

23.	Licencje	Przełącznik musi być dostarczony z licencją umożliwiającą pracę portów przełącznika z prędkością 16 Gb/s Przełącznik FC musi posiadać wszystkie porty FC aktywne.
24.	Wymagania formalne	a) Oferowany przez Wykonawcę i dostarczony Sprzęt musi być fabrycznie nowy, nigdy wcześniej nieużywany i wyprodukowany maksymalnie 6 miesięcy przed dniem poprzedzającym złożenie oferty. b) Przełączniki i wszystkie komponenty muszą pochodzić z seryjnej produkcji. c) Oferowane przez Wykonawcę elementy dotyczące rozbudowy przełączników takie jak: wkładki muszą znajdować się na liście elementów kompatybilnych producenta dostarczonych przełączników i nie mogą powodować utraty gwarancji.
25.	Warunki serwisu i gwarancji	a) Przełączniki muszą posiadać pakiet usług gwarancyjnych kierowanych do użytkowników z obszaru Rzeczypospolitej Polskiej oparty na gwarancji. Wykonawca zobowiązany jest przedstawić Zamawiającemu w momencie zawarcia umowy dokument potwierdzający realizację wymagania. W przypadku, gdy dokument został wystawiony w języku innym niż polski należy je przetłumaczyć na język polski (Wykonawca potwierdza dokument za zgodność z oryginałem). b) Czas trwania serwisu gwarancyjnego sprzętu wynosi nie mniej niż 36 miesięcy, liczony od dnia podpisania protokołu odbiór przedmiotu zamówienia wnioskującego o rozliczenie finansowe. c) Wymaga się, aby usługi gwarancyjne świadczone były w następujących trybach: - czas reakcji w formule NBD - czas naprawy awarii nie może być dłuższy niż 5 dni. - czas gwarancji – zgodnie z OPZ. d) Obsługa serwisowa w języku polskim, e) Wykonawca w ramach serwisu gwarancyjnego zapewni aktualizację, konfigurację i rekonfigurację . W ramach serwisu gwarancyjnego Wykonawca wyznaczy dedykowanego specjalistę, spośród specjalistów wskazanych do realizacji zamówienia w Wykazie osób złożonym z ofertą, który będzie odpowiedzialny za realizację usług w zakresie serwisu gwarancyjnego, a także za przekazywanie oraz otrzymywanie informacji i komentarzy zwrotnych dotyczących usług gwarancyjnych. f) W przypadku zmian w konfiguracji Wykonawca opracuje dokumentację techniczną zawierającą przebieg tych prac. Dokumentacja ta będzie zawierać konfigurację Sprzętu przed wprowadzeniem zmian, czynności wykonywane w trakcie rekonfiguracji oraz konfigurację Sprzętu po wprowadzeniu zmian.
26.	Usługi	Usługa montażu, integracji i konfiguracji funkcji przełączników w miejscu wskazanym przez zamawiającego, zgodnie z ich specyfikacją. Dokładny zakres wdrożenia zostanie ustalony na etapie realizacji z zamawiającym i będzie składał się z dowolnych wymagań zawartych w OPZ.

Dla elementów, dla których nie zostały określone warunki gwarancji, obowiązują **Podstawowe warunki gwarancji określone w punkcie 3.4. OPZ.**

* Warunki równoważności na dostarczane oprogramowanie

Zamawiający uzna, że zaoferowane rozwiązanie posiada równoważne cechy z przedmiotem zamówienia, jeżeli będzie ono zawierało funkcjonalności co najmniej tożsame lub lepsze od określonych w niniejszym opisie przedmiotu zamówienia w zakresie posiadanej funkcjonalności i będzie kompatybilne w 100% z oprogramowaniem posiadanym przez Zamawiającego, o którym mowa w niniejszym opisie przedmiotu zamówienia. W przypadku zaproponowania wersji równoważnej Wykonawca zobowiązany jest przedstawić na żądanie Zamawiającego opis i dane techniczne zaproponowanego rozwiązania umożliwiające porównanie go z wszystkimi parametrami wymaganymi niniejszym opisem przedmiotu zamówienia w tym zgodność posiadanego oprogramowania z zaproponowanym rozwiązaniem. Dodatkowo Zamawiający zastrzega sobie prawo do zweryfikowania funkcjonalności, wydajności i kompatybilności zaoferowanego rozwiązania równoważnego poprzez analizę jego możliwości. W przypadku skorzystania przez Zamawiającego z ww. uprawnienia wykonawca jest zobowiązany w terminie 5 dni od dnia otrzymania od Zamawiającego wezwania do dostarczenia testowej wersji zaproponowanego rozwiązania dostarczyć to rozwiązanie do siedziby Zamawiającego.

Za rozwiązanie równoważne Zamawiający uznaje rozwiązanie, które nie spowoduje poniesienia dodatkowych kosztów (np. dodatkowych licencji, dodatkowego sprzętu, kosztów związanych z modyfikacją systemów działających u Zamawiającego, itp.) po stronie Zamawiającego.