

Załącznik nr 4 do SIWZ

Znak sprawy: DZP.271.5.2020

OPIS PRZEDMIOTU ZAMÓWIENIA

Adaptacja i wyposażenie dwóch serwerowni

w ramach projektu

Śląska Cyfrowa Platforma Medyczna eCareMed

Projekt finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego (EFRR) w ramach Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2014 – 2020, II Osi Priorytetowej „CYFROWE ŚLĄSKIE”, Działanie 2.1 „Wsparcie rozwoju cyfrowych usług publicznych”.

I. ZAKRES ROBÓT

1. Kod i nazwa kodu CPV

45311000-0 – Roboty w zakresie okablowania oraz instalacji elektrycznych
45312100-8 – Instalowanie przeciwpożarowych systemów alarmowych
45331000-6 – Instalowanie urządzeń grzewczych, wentylacyjnych i klimatyzacyjnych
45400000-1 – Roboty wykończeniowe w zakresie obiektów budowlanych
45421131-1 – Instalowanie drzwi
45450000-6 – Roboty budowlane wykończeniowe pozostałe

2. Zakres rzeczowy przedmiotu zamówienia

W związku z planowanym wytworzeniem i uruchomieniem usług dostępnych przez sieć Internet (e-usług) stanowiących integralną część platformy wytworzonej w ramach projektu eCareMed_P4 „Śląska Cyfrowa Platforma Medyczna eCareMed”, wymagane jest dostosowanie istniejącej infrastruktury technicznej Beskidzkiego Centrum Onkologii -Szpital Miejski w celu zapewnienia odpowiednich, zgodnych z powszechnie obowiązującymi standardami, warunki pracy sprzętu serwerowego oraz zapewnienia odpowiednio wysokiego poziomu bezpieczeństwa przetwarzania danych.

Niniejsze zadanie dotyczy uruchomienia dwóch w pełni funkcjonalnych serwerowni zlokalizowanych na terenie szpitala:

- Głównego Centrum Przetwarzania Danych (GCPD)
- Zapasowego Centrum Przetwarzania Danych (ZCPD)

W ramach adaptacji i wyposażenia Głównego Centrum Przetwarzania Danych zostaną wykonane dostawy wyposażenia oraz prace adaptacyjne wymienione poniżej:

- 1) Dostawa , montaż pięciu szaf serwerowych RACK.
- 2) Dostawa i montaż systemu klimatyzacji.
- 3) Dostawa , montaż i uruchomienie systemu sygnalizacji i gaszenia pożaru.
- 4) Dostawa, montaż i uruchomienie zasilacza awaryjnego.
- 5) Dostawa, montaż i uruchomienie systemu monitoringu wizyjnego.
- 6) Dostawa, montaż i uruchomienie systemu kontroli dostępu.
- 7) Dostawa, montaż i konfiguracja urządzenia brzegowego klasy UTM
- 8) Ułożenie i wykonanie połączeń kabla światłowodowego wewnątrz budynku GCPD (serwerownia)

W ramach adaptacji i wyposażenia Zapasowego Centrum Przetwarzania Danych zostaną wykonane dostawy urządzeń wraz z konieczną ich instalacją:

- 1) Dostawa, montaż trzech szaf serwerowych RACK.
- 2) Dostawa , montaż i uruchomienie systemu klimatyzacji.
- 3) Dostawę , montaż i uruchomienie systemu sygnalizacji i gaszenia pożaru.
- 4) Dostawa, montaż i uruchomienie systemu monitoringu wizyjnego.
- 5) Dostawa, montaż i uruchomienie systemu kontroli dostępu.

Ponadto Zamawiający wymaga wykonanie następujących prac

- 1) Dostawa, montaż i uruchomienie zasilacza awaryjnego
- 2) Demontaż instalacji centralnego ogrzewania.
- 3) Demontaż istniejących drzwi do pomieszczenia ZCPD.
- 4) Montaż drzwi wejściowych antywłamaniowych, o podwyższonej odporności ogniowej.

- 5) Malowanie i zabezpieczenie ścian w klasie odporności ogniowej 60 min.
- 6) Wykonanie zabezpieczenia okien - Zamawiający dopuszcza demontaż stolarki okiennej i zamurowanie otworu okiennego.
- 7) Wykonanie projektu elektrycznego zasilania ZCPD.
- 8) Wykonanie instalacji elektrycznych zgodnie z wcześniej wykonanym projektem elektrycznym.
- 9) Wykonanie systemu uziemień i połączeń wyrównawczych.
- 10) Ułożenie kabla zasilającego z rozdzielni zlokalizowanej w budynku głównym do pomieszczenia ZCPD- zgodnie z wcześniej wykonanym projektem elektrycznym.
- 11) Ułożenie i wykonanie połączeń kabla światłowodowego wewnątrz budynku głównego od złącza zlokalizowanego przy pomieszczeniu Statystyki do ZCPD.

Okablowanie światłowodowej sieci LAN pozwalającą na wymianę danych pomiędzy Głównym Centrum Przetwarzania Danych i Zapasowym Centrum Przetwarzania Danych zostanie wykonane w nowych korytach kablowych przez Wykonawcę realizującego rozbudowę BCO-SM zgodnie z rysunkiem - załącznik nr 7 do SWIZ.

Zamawiający wymaga, przed przystąpieniem do prac instalacyjnych, dostarczenie projektu wykonawczego instalacji zasilania elektrycznego, systemu klimatyzacji, instalacji teletechnicznych oraz koncepcji rozmieszczenia i wykonania pomieszczeń serwerowni w obu ośrodkach przetwarzania danych. Dokumentacja projektowa musi uwzględniać wytyczne OPZ oraz być zaakceptowana przez Zamawiającego.

Na etapie przygotowania dokumentacji projektowej należy dokonać weryfikacji istniejących instalacji teletechnicznych i dokonać szerokiej konsultacji z Zamawiającym. Przeprowadzone konsultacje powinny dotyczyć uzgodnień technicznych w zakresie ostatecznej lokalizacji szaf serwerowych, systemu klimatyzacji, przyłączy elektrycznych i teletechnicznych oraz sposobu przyszłego prowadzenia prac.

Przed przystąpieniem do realizacji Zamawiający zaleca zapoznanie się z terenem Szpitala oraz pomieszczeniami, w których zostanie utworzone GCPD oraz ZCPD.

W zakresie niezbędnym do wykonania dokumentacji Zamawiający udostępni dostęp do pomieszczeń, infrastruktury technicznej i wyposażenie które będą konieczne do wykonania dokumentacji.

Zamawiający udostępni wszelkie pozostające w jego dyspozycji dokumenty i informacje dotyczące nieruchomości, budynków oraz jego wyposażenia w zakresie projektowanej sieci. Brakujące dokumenty, informacje i rysunki niezbędne do wykonania dokumentacji Wykonawca uzupełni własnym staraniem.

W trakcie wizji lokalnych Wykonawca na własny koszt dokona inwentaryzacji przekazanych kserokopii projektów i dokumentów i w poprawnej wersji użyje do celów projektowych.

Koordinacja robót budowlano-montażowych poszczególnych rodzajów powinna być dokonana we wszystkich fazach procesu budowy. Koordinacją należy objąć projekt organizacji budowy, szczegółowy harmonogram robót instalacyjnych oraz pomocnicze roboty ogólnobudowlane związane z realizacją ZCPD.

Wszystkie stosowane materiały i urządzenia muszą być fabrycznie nowe i dobrej jakości, a także muszą dokładnie odpowiadać warunkom niezbędnym do prawidłowego wykonania powierzonych robót oraz do poprawnego funkcjonowania całej instalacji. Stosowane materiały i urządzenia muszą posiadać wymagane deklaracje zgodności lub certyfikaty dopuszczające do stosowania ich w budownictwie.

Wszelkie uszkodzenia infrastruktury ogólnej w obiekcie przez Wykonawcę podczas prowadzenia prac instalacyjnych obciążają jego samego i muszą być usunięte w ramach nieodpłatnego usunięcia szkód w terminie niezwłocznym po ich wykonaniu,

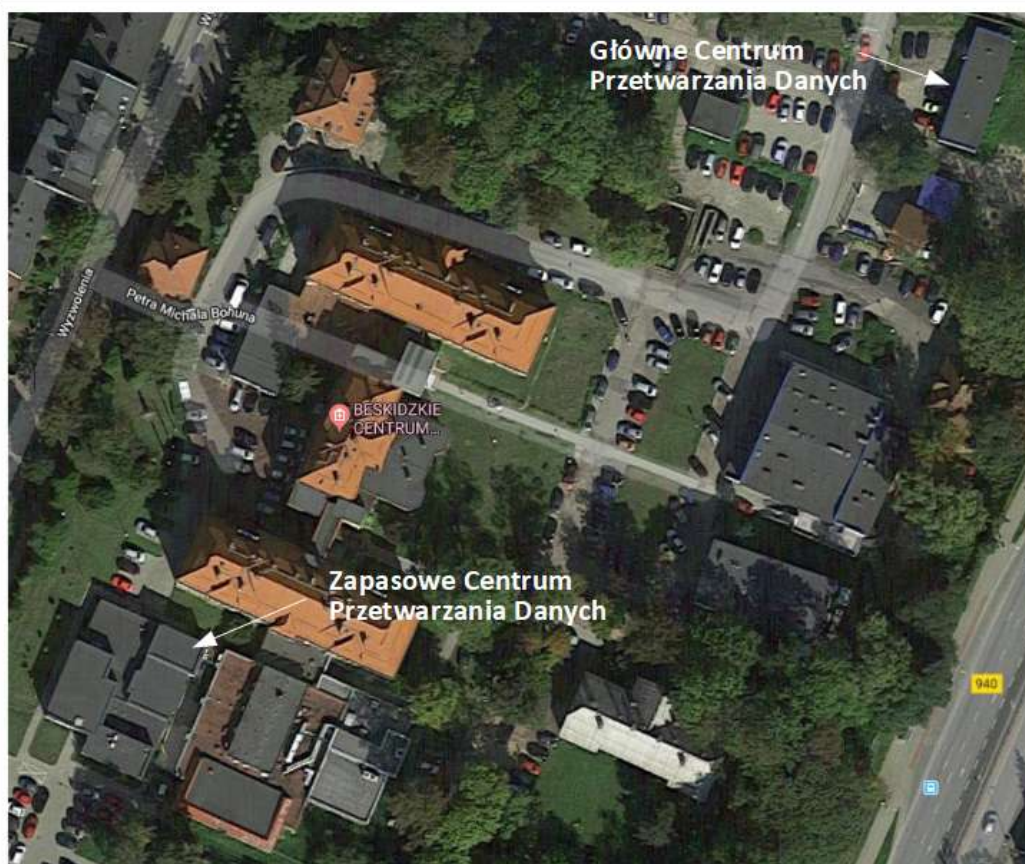
Zamawiający wymaga, aby odpady powstałe w wyniku realizowanych prac instalacyjnych, narzędzia i inne przedmioty były każdorazowo uprzątnięte z ciągów komunikacyjnych i z biur do godz. 7:00 rano tak aby umożliwiały bezpieczne wykonywanie pracy,

Wykonawca zobowiązany jest do pozostawienia pomieszczeń w których będą wykonywane prace w stanie takim jaki zastał przed przystąpieniem do prac.

3. Aktualne uwarunkowania wykonania przedmiotu zamówienia

Prace adaptacyjne będą wykonywane w pomieszczeniach zlokalizowanych w dwóch odrębnych budynkach oddalonych od siebie około 300 m w linii prostej:

- 1) Główne Centrum Przetwarzania Danych w budynku obecnej serwerowni.
- 2) Zapasowe Centrum Przetwarzania Danych w budynku radioterapii.



Budynki nie są objęte opieką konserwatora, a Zamawiający posiada prawo dysponowania wraz z wpisem do Księgi wieczystej.

Główne Centrum Przetwarzania Danych powstanie w istniejącym budynku serwerowni, w którym rozpoczęto główne prace adaptacyjne wydzielając od zaplecza i pomieszczeń technicznych, pomieszczenie o powierzchni 23 m² na cele serwerowni, zgodnie z planem będącym załącznikiem nr 9 do SIWZ.

Zapasowe Centrum Przetwarzania Danych zostanie utworzone w budynku TELERADIOTERAPII na parterze w pomieszczeniu o powierzchni ok. 15m² oznaczonym na planie kondygnacji (załącznik nr 5 do SIWZ) jako **Pokój Kierownika**.

4. Szczególne uwarunkowania związane z wykonaniem zamówienia

W budynkach, w którym będą wykonywane prace instalacyjno-montażowe pełnią funkcję administracyjno – biurową w przypadku GCPD oraz funkcję leczniczą w przypadku ZCPD i będą użytkowane w trakcie realizacji Zamówienia,

Prowadzenie prac w trakcie pracy szpitala jest możliwe, ale tak aby nie zakłócać jego funkcjonowania i prowadzić do dyskomfortu pracy pracowników oraz pacjentów Szpitala. Prace w tym okresie będą mogły być prowadzone po przekazaniu zasad wykonywania prac w tym okresie i zgody wydanej przez upoważnioną osobę ze strony Zamawiającego,

Dopuszcza się pracę w dni robocze w godzinach od 7.30 do 18.00

Wstęp, zasady poruszania i wykonywania prac w budynkach Szpitala przez pracowników Wykonawcy poza normalnymi godzinami pracy Szpitala będzie możliwy po przekazaniu zasad wykonywania prac w tym okresie i zgody wydanej przez upoważnioną osobę ze strony Zamawiającego.

Miejsca jak i urządzenia w których Wykonawca będzie wykonywał prace będą musiały być skutecznie zabezpieczone przed zabrudzeniem, zapyleniem, uszkodzeniem, zniszczeniem. Koszty związane potencjalnymi stratami w tym zakresie Wykonawca ponosi we własnym zakresie i jednocześnie zobowiązuje się że stan Szpitala i zainstalowanych urządzeń nie będzie gorszy niż przed rozpoczęciem prac,

Wykonawca będzie przestrzegał wszystkich związanych z wykonywanymi pracami przepisów BHP.

Zamawiający będzie wymagał od wykonawcy na każdym etapie prac instalacyjnych w GCPD szerokiej konsultacji dotyczącej terminu i sposobu realizacji etapu zadania, celem koordynacji z innymi pracami realizowanymi w ramach odrębnego postępowania na obiekcie i w jego otoczeniu.

Wszelkie uszkodzenia infrastruktury ogólnej w obiekcie przez Wykonawcę podczas prowadzenia prac instalacyjnych obciążają jego samego i muszą być usunięte w ramach nieodpłatnego usunięcia szkód w terminie niezwłocznym po ich wykonaniu.

Dostarczone na miejsce budowy materiały należy sprawdzić pod względem ilości, kompletności i zgodności z danymi wytwórcy. Każdą dostawę towaru na budowę należy potwierdzić pisemnie.

W przypadku stwierdzenia niezgodności, wad lub nasuwających się wątpliwości mogących mieć wpływ na jakość wykonania robót, należy skontaktować się z dostawcą i wyjaśnić zaistniałe wątpliwości, a materiały przed ich zabudowaniem poddać badaniom określonym przez dozór techniczny ze strony producenta lub wykonawcy robót.

Składowanie materiałów powinno odbywać się w warunkach zapobiegających zniszczeniu, uszkodzeniu lub pogorszeniu się właściwości technicznych na skutek wpływu czynników atmosferycznych lub fizykochemicznych. Należy zachować wymagania wynikające ze specjalnych właściwości materiałów oraz wymagania w zakresie bezpieczeństwa przeciwpożarowego. Należy zastosować się do zaleceń producenta w w/w zakresie.

Wszystkie stosowane materiały i urządzenia muszą być fabrycznie nowe i dobrej jakości, a także muszą dokładnie odpowiadać warunkom niezbędnym do prawidłowego wykonania powierzonych robót oraz do poprawnego funkcjonowania całej instalacji. Stosowane materiały i urządzenia muszą posiadać wymagane deklaracje zgodności lub certyfikaty dopuszczające do stosowania ich w budownictwie.

Urządzenia i sprzęt zmechanizowany podlegające przepisom o dozorze technicznym, eksploatowane na budowie, powinny mieć aktualnie ważne dokumenty uprawniające do ich eksploatacji.

Informacje i dokumenty niezbędne do wykonania dokumentacji projektowej:

- 1) Dokumentacja projektowa musi być zgodna z:

- ustawą z dnia 7.07.1994 Prawo budowlane (Dz.U. 2018 poz. 1202, z późn. zm.) oraz przepisami wykonawczymi do tej ustawy;
 - rozporządzeniem Ministra Infrastruktury z dnia 02.09. 2004r. w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych... (Dz.U. 2012 poz.365);
 - normą branżową PN-IEC 60364 – Instalacje elektryczne w obiektach budowlanych;
- 2) Wykonawca będzie ponosił wyłączną i pełną odpowiedzialność za treść dokumentacji projektowej, uzgodnione i własne założenia dokonane na potrzeby jej wykonania;
 - 3) Zamawiający udostępni wszelkie pozostające w jego dyspozycji dokumenty i informacje dotyczące nieruchomości, budynków oraz jego wyposażenia w zakresie projektowanej sieci. Brakujące dokumenty, informacje i rysunki niezbędne do wykonania dokumentacji Wykonawca uzupełni własnym staraniem;
 - 4) W trakcie wizji lokalnych Wykonawca na własny koszt dokona inwentaryzacji przekazanych kserokopii projektów i dokumentów i w poprawnej wersji użyje do celów projektowych;
 - 5) W zakresie niezbędnym do wykonania dokumentacji Zamawiający udostępni dostęp do pomieszczeń, infrastruktury technicznej i wyposażenie które będą konieczne do wykonania dokumentacji;
 - 6) Jeżeli okaże się to konieczne to Zamawiający wystawi pełnomocnictwo do reprezentowania Zamawiającego przed organami administracji państwowej i samorządowej oraz instytucji opiniującymi we wszystkich sprawach związanych z wykonaniem dokumentacji projektowej z zastrzeżeniem że koszty uzyskania niezbędnych dokumentów, odpowiednich decyzji, postanowień i uzgodnień będzie ponosił Wykonawca;
 - 7) Budynek dla których będą wykonywane projekty nie jest wpisany do rejestru zabytków i nie podlegają pod Konserwatora Zabytków;
 - 8) Budynek posiadają zasilanie energetyczne. Zamawiający na etapie wykonywania dokumentacji elektrycznej dokona analizy związanej z przebudową instalacji elektrycznej i podejmie decyzje w sprawie czy są konieczne zmiany w energetycznej instalacji przyłączeniowej, jak i zmiany przydziału mocy dla budynków.

II. RÓWNOWAŻNOŚĆ ROZWIĄZAŃ

W celu zachowania reguły konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych w treści niniejszego OPZ, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności przez to rozwiązanie oferowanych, nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym.

Materiały lub urządzenia pochodzące od konkretnych producentów stanowią wyłącznie wzorec jakościowy przedmiotu zamówienia. Pod pojęciem minimalne parametry jakościowe i cechy użytkowe Zamawiający rozumie wymagania dotyczące materiałów lub urządzeń zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach pod względem:

- a) gabarytów i konstrukcji (wielkość, rodzaj, właściwości fizyczne, liczba elementów składowych),
- b) charakteru użytkowego (tożsamość funkcji),
- c) charakterystyki materiałowej (rodzaj i jakość materiałów),
- d) parametrów technicznych (wytrzymałość, trwałość, dane techniczne, dane hydrauliczne, charakterystyki linowe, konstrukcja),
- e) parametrów bezpieczeństwa użytkowania,
- f) standardów emisyjnych.

W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób. Za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, identycznych dla obu rozwiązań, dla których to warunków rozwiązania te są dedykowane.

Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, iż spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.

III. GWARANCJA

Wykonawca udzieli 5-cio letniej gwarancji na przedmiot umowy, na warunkach zgodnie z wymaganiami określonymi w Opisie Przedmiotu Zamówienia, realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez linię telefoniczną producenta lub autoryzowanej firmy serwisującej.

Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia.

Urządzenia muszą być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.

Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie kraju sprzedaży.

IV. OZNACZENIE CE

Wszystkie rozwiązania dostarczone w ramach zadania muszą posiadać deklarację zgodności CE lub równoważną.

W przypadku braku deklaracji zgodności CE na internetowych stronach producenta, Zamawiający wymaga złożenia wraz z ofertą dokumentów potwierdzających spełnienie przez produkt w/w wymagań jakościowych.

V. MINIMALNE WYMAGANIA DLA ROBÓT I DOSTAW

1. Główne Centrum Przetwarzania Danych

1.1. Wymagania ogólne

Dla potrzeb Głównego Centrum Przetwarzania Danych Zamawiający wymaga dostawy wraz z montażem i uruchomieniem modułowego systemu szaf szczelnych zintegrowanych z systemem klimatyzacji precyzyjnej w oparciu o wymiennik woda-powietrze, składającego się z minimum:

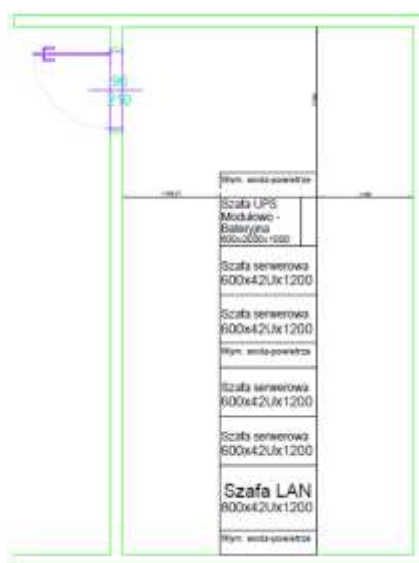
- 4 szaf serwerowych typu RACK 19" o wymiarach 600x1200x42U,
- 1 szafy na infrastrukturę LAN typu RACK 19" o wymiarach 800x1200x42U,
- 1 szafy na potrzeby zasilania awaryjnego UPS,
- zintegrowanego systemu klimatyzacji międzrzędowej,
- zintegrowanego systemu sygnalizacji i gaszenia pożaru.

Przed montażem w/w urządzeń, Zamawiający wymaga wykonanie projektu instalacji systemu chłodzenia opartego, w którym czynnikiem chłodzącym będzie woda z domieszką glikolu. Ilość i rozmieszczenie modułów systemu klimatyzacji musi zapewnić optymalne warunki chłodzenia dla wszystkich szaf systemu.

Projekt wykonawczy musi zawierać co najmniej:

- Opis rozwiązania,
- Rysunki (plany) lokalizacji głównych elementów instalacji, prowadzenie instalacji, rysunki elementów systemu, rysunki przyłącza agregatu, schematy blokowe – potrzebne wykonawcy do realizacji zadania,
- Sposób wykonania pomiarów - w projekcie wykonawczym należy zawrzeć warunek wykonania pomiarów torów transmisyjnych linii światłowodowych,
- Specyfikację materiałową,
- Specyfikację techniczną budowy i odbioru robót,
- Informację dotyczącą bezpieczeństwa i ochrony zdrowia

Ze względu na ograniczenia powierzchni GCPD, moduły należy montować w układzie jednorzędowym zgodnie przykładowym schematem rozmieszczenia szaf.



Zamawiający dopuszcza zmianę układu rozmieszczenia szaf w rzędzie oraz ilości i układu wymienników ciepła w celu zapewnienia optymalnych warunków chłodzenia oferowanego rozwiązania pod warunkiem wcześniejszej konsultacji i akceptacji przez Zamawiającego.

System szaf szczelnych klimatyzowanych musi być dostarczony wraz z systemem zarządzania infrastrukturą serwerowni i monitorowania warunków fizycznych.

Dla kluczowych elementów systemu szaf:

- zasilania awaryjnego UPS,
- listew dystrybucji zasilania PDU,
- systemu wczesnego wykrywania i gaszenia pożaru,
- systemu automatycznego awaryjnego otwarcia drzwi szaf,
- zintegrowanego systemu klimatyzacji,

należy zastosować system umożliwiający komunikację urządzeń, zdalną kontrolę i zarządzanie urządzeniami.

W ramach przygotowywania pomieszczenia Główne Centrum Przetwarzania Danych do realizacji zadań należy wykonać instalację, konfigurację systemu kontroli dostępu do pomieszczeń. Jeżeli pomieszczenia będzie wymagało dostosowania – okablowanie sieci LAN, zasilanie, uchwyty itp. – Wykonawca powinien to uwzględnić w swojej ofercie. Oferta powinna zawierać także wycenę prac instalacji i konfiguracji systemu monitoringu również uwzględniając konieczne elementy – okablowanie, uchwyty, koryta kablowe i inne elementy instalacyjne -wszystkie użyte do instalacji elementy winny posiadać odpowiednie atesty i być zaakceptowane przez Zamawiającego..

System bezpieczeństwa – system kontroli dostępu, system monitoringu wizyjnego – po realizacji usługi instalacji i konfiguracji musi w celu odbioru prac realizować wszystkie wymagane od systemów funkcje.

1.2. Szafy RACK 19"

Nazwa komponentu	Wymagane minimalne
WYMAGANIA OGÓLNE	<p>Stelaż szaf musi być wykonany ze spawanej ramy odpornej na skręcanie, o nośności minimum 1500 kg.</p> <p>Płaszczyna montażowa 19" musi składać się z uniwersalnych szyn profilowych do zastosowań serwerowych, sieciowych i elektronicznych.</p> <p>Szyny profilowe z tyłu muszą być przygotowane do obustronnego zamocowania list zasilających PDU (Power Distribution Unit) w przestrzeni 0 U.</p> <p>Elementy szafy wykonane z blachy stalowej lub aluminium, malowane proszkowo w kolorze RAL.</p> <p>Szafy muszą być szczelne, przystosowane do systemów chłodzenia wewnętrznego (w obrysie szafy) współpracującego z agregatem chłodniczym.</p>
DRZWI	<p>Przednie drzwi przeszklone z szybą wykonaną ze szkła hartowanego o szczelności na poziomie IP54, wyposażone w zamek dźwigienkowy.</p> <p>Drzwi muszą być wyposażone w systemową kontrolę dostępu, zapewniającą współpracę z zastosowanymi wymiennikami ciepła powietrze woda oraz muszą współpracować z systemem automatycznego awaryjnego otwarcia drzwi szaf.</p>

	Tylnie drzwi pełne z blachy stalowej, zamykane na zamek.
PŁYTA DACHOWA	Możliwość bocznego wprowadzania kabli przez listwy szczotkowe. Możliwość instalacji wentylatorów.
PŁYTA PODŁOGOWA	Płyta podłogowa przygotowana na przepusty piankowe pozwalająca na wprowadzenie kabli przy zachowaniu zakładanej szczelności szafy. Wszystkie skręcone części poszycia podłogi z automatycznym wyrównaniem potencjałów i przygotowaniem do mocowania taśm uziemienia.
WYPOSAŻENIE PODSTAWOWE	Każda szafa serwerowa musi być wyposażona w minimum: <ul style="list-style-type: none"> – pionowe prowadnice powietrza do rozdzielania stref ciepłego i zimnego powietrza wew. szczelnie zamkniętej i chłodzonej wew. szafy w separacji; – panel porządkujący wraz z minimum pięcioma wieszakami stalowymi; – 8 stalowych ocynkowanych lub malowanych proszkowo szyn montażowych poziomych, montowane po głębokości szaf 1200mm po 4 szt. na lewą i prawą stronę; – 10 szt. kablowych wieszaków przelotowych do elastycznego i uporządkowanego prowadzenia okablowania, bocznie na szynach profilowych; – boczny kanał kablowy pozwalający na prowadzenie okablowania w pionie oraz przeprowadzenie kabli do wnętrza szafy; – 3 szt. 19" paneli zaślepiających 3U do zamknięcia wolnych obszarów. Zamawiający wymaga zaślepienia wszystkich wolnych miejsc frontu szafy. Przeliczenie docelowej ilości paneli zaślepiających pozostaje po stronie wykonawcy;
LISTWY ZASILAJĄCE PDU	Szafy serwerowe oraz na infrastrukturę LAN muszą posiadać po minimum dwie pionowe listwy zasilające PDU 400V 50/60 Hz, opomiarowane na każdą z faz z podłączeniem do sieci zdalnego monitorowania. Listwy PDU muszą posiadać możliwość montażu w przestrzeni pomiędzy ścianą boczną a profilem 19" w dedykowanych zatokach szafy przeznaczonych na dystrybucję zasilania oraz alternatywnie po dwie bliźniaczo, na stronę lewą lub prawą. Minimalna ilość i typ gniazd EN 60320: 18 x C13, 4 x C19. Funkcje pomiarowe: Napięcie (V) w zakresie 90V-250V, prąd (A) w zakresie 0,1A-16A, częstotliwość (Hz), Moc czynna (kW), praca czynna (kWh), moc bierna, Współczynnik mocy (cos Ø), moc pozorna (VA). Możliwość zdalnego monitorowania z wykorzystaniem protokołów http, HTTPS, SSL, SSH oraz usługi Telnet. Obsługiwane protokoły komunikacyjne: TCP/IP, SNMP, FTP/SFTP. Możliwość podłączenia do każdego PDU czujników monitoringu: czujnik temperatury, czujnik temperatury / wilgotności.
MONITORING INFRASTRUKTURY I WARUNKÓW ŚRODOWISKOWYCH	Szafy muszą być wyposażone w system monitoringu infrastruktury fizycznej pozwalający na: <ul style="list-style-type: none"> – pomiar temperatury w szczelnie zamkniętych szafach w zakresie 10°C – 50°C;

	<p>– pomiar wilgotności w szczelnie zamkniętych szafach w zakresie 10% - 95%.</p> <p>System monitoringu musi być dostarczony z czujnikami umożliwiającymi pomiar temperatury i wilgotności oraz czujnik wykrywający wyciek w pomieszczeniu serwerowni. Wymagane są podziały wykrycia wycieku na strefy od 1 do 5 na długości max. 15m.</p> <p>System musi umożliwiać monitorowanie parametrów fizycznych wyodrębnionych elementów całościowego systemu infrastruktury IT za pomocą protokołu CAN-Bus: listew dystrybucji zasilania PDU, systemu wczesnego wykrywania i gaszenia pożaru w szafach zamkniętych, klimatyzacji międzyszafowej opartej na systemie schładzanej wody z glikolem, agregatów chłodzenia cieczy IT, systemu szaf zasilania awaryjnego UPS.</p> <p>System musi umożliwiać zdalny monitoring paneli gaśniczych 19”.</p> <p>System musi umożliwiać zdalny monitoring i sterowanie dla automatycznego awaryjnego otwarcia drzwi szaf.</p> <p>Musi umożliwiać monitoring i zarządzanie zdalne listwami dystrybucji energii PDU.</p> <p>Obsługiwane protokoły: TCP/IP, SNMPv1, SNMPv2c, SNMPv3, SSH, FTP, SFTP, HTTP, HTTPS, NTP, DHCP, DNS, SMTP, XML*, Syslog.</p> <p>Musi umożliwiać równoległą do SNMP możliwość komunikacji z centralnym modułem monitorowania za pomocą protokołu Modbus TCP IP.</p> <p>System musi być wyposażony w zegar czasu rzeczywistego z NT.</p> <p>System musi umożliwiać zdalną kontrolę i zarządzania.</p> <p>System musi umożliwiać współpracę z przewidzianym modułem GSM 4G pozwalającym na alternatywne powiadomienia alarmowe, ostrzeżenia komunikatem SMS.</p>
AUTOMATYCZNE AWARYJNE OTWIERANIE DRZWI	<p>Każda szafa musi być wyposażona w system automatycznego awaryjnego otwarcia drzwi przednich i tylnych.</p> <p>System automatycznego awaryjnego otwarcia drzwi musi automatycznie otwierać drzwi szaf w przypadku braku zasilania oraz awarii układu chłodzenia.</p>

1.3. System zasilania awaryjnego UPS

Nazwa komponentu	Wymagane minimalne
WYMAGANIA OGÓLNE	<p>System zasilania awaryjnego UPS musi być dostarczony w formie rozwiązania modułowego, zainstalowanego w wydzielonej szafie zasilania awaryjnego 19” typu RACK przystosowanej do chłodzenia przez wymiennik woda / powietrze, zintegrowanej z zespołem szaf serwerowych.</p> <p>Modułowy system zasilania awaryjnego musi zapewniać min. 60kW mocy czynnej. Moduły muszą być autonomiczne z własnym systemem sterowania i obciążenia (przetątnik obciążeniowy).</p> <p>Szafa na moduły mocy musi zapewniać możliwość rozbudowy.</p> <p>Szafa zasilania awaryjnego musi być szczelnie zamknięta i przystosowana</p>

	<p>do gaszenia panelami 19" wczesnego wykrywania i gaszenia pożaru wraz z integrowanym systemem awaryjnego i automatycznego otwierania drzwi przednich i tylnych szaf w przypadku awarii układu chłodzenia.</p> <p>Projektowany UPS musi posiadać kartę SNMP oraz wspólny system monitorowania i zarządzania jak wymienniki ciepła powietrze / woda, agregat chłodzenia cieczy, system dystrybucji energii w szafach PDU, system centralnego monitorowania parametrów fizycznych w obrębi projektowanej serwerowni, system automatycznego awaryjnego otwarcia drzwi szaf, system wczesnego wykrywania i gaszenia pożaru w szafach.</p> <p>Do projektowanego systemu zasilania awaryjnego UPS należy podłączyć minimum agregat chłodzenia cieczy poprzez specjalne dedykowane w nim złącze zasilania UPS. Pozostałe elementy infrastruktury chłodzenia muszą posiadać gwarantowane źródło zasilania niezależnie.</p>
FUNKCJONALNOŚĆ	<p>Moduły UPS muszą być wyposażone w wyświetlacz LCD do obsługi systemu, umożliwiający sterowanie systemem oraz dostęp do rejestru zdarzeń i do trybu serwisowego. Wyświetlacz musi posiadać wskaźnik przepływu prądu oraz wskaźnik pracy.</p> <p>Na wyświetlaczu musi być podawana moc czynna, pozorna i bierna.</p> <p>System UPS musi dysponować automatycznym testem baterii, uruchamianym regularnie w dowolnie zaprogramowanych odstępach czasu. Wymagane są baterie stacjonarne, zamknięte bezobsługowo, ołowiowe z rekombinacją gazów.</p> <p>Ładowanie baterii bez falistości prądu przemiennego przez rozdzielanie ładowarki DC-DC od prostownika i falownika.</p> <p>Zabezpieczenie przed rozładowaniem baterii przy skokach obciążenia.</p> <p>Możliwość przejęcia jednego i tego samego obciążenia przez kilka modułów UPS w redundantnej konfiguracji równoległej.</p>
Moc	<p>Znamionowa 20 kV / 20 kW każdy moduł bateryjny</p> <p>Minimalna moc: 60 kW</p>
WEJŚCIE	<p>Napięcie: 3 x 400/230 V</p> <p>Częstotliwość sieciowa: 50 Hz</p> <p>Zakres częstotliwości bez rozładowania baterii: 40 - 70 Hz</p> <p>THDI: < 3%</p> <p>Współczynnik mocy wejściowej: ≥ 0,99</p>
WYJŚCIE	<p>Napięcie: 400/230V</p> <p>Częstotliwość: 50Hz</p> <p>Przebieżalność: minimum 125%/10min</p> <p>Sprawność przy obciążeniu liniowym >75%: ≥95%</p>
TYP BATERII	VRLA lub równoważny
CZAS PODTRZYMANIA BATERyjNEGO	minimum 10 minut
INNE	<p>Osobne zasilanie dla obejścia i prostownika.</p> <p>Złącza: RS-232, USB.</p> <p>Oprogramowanie do zarządzania urządzeniem.</p>

1.4. Zintegrowany system klimatyzacji

Nazwa komponentu	Wymagane minimalne
WYMAGANIA OGÓLNE	<p>System klimatyzacji musi zapewnić chłodzenie wszystkich dostarczonych szaf przy uwzględnieniu ich nominalnego wyposażenia i obciążenia cieplnego.</p> <p>W celu zapewnienia optymalnego chłodzenia urządzeń dla szczelnie zamkniętych szaf należy zaprojektować min. dwa klimatyzatory międzyrzędowe typu wymiennik ciepła powietrze/ woda zintegrowane z szafami serwerowymi.</p> <p>Dodatkowo zestaw szaf zasilacza awaryjnego musi zostać wyposażony w minimum jeden wymiennik ciepła powietrze/ woda.</p> <p>Musi współpracować z agregatem wody lodowej.</p> <p>Prowadzenie powietrza musi opierać się na zasadzie chłodzenia wbudowanych w szafie urządzeń "front to back".</p> <p>Regulacja temperatury wdmuchiwanego zimnego powietrza musi odbywać się poprzez stałe wyrównanie temperatury rzeczywistej z temperaturą zadaną na wymienniku ciepła.</p>
CZYNNIK CHŁODNICZY	Woda lodowa.
MOC KLIMATYZATORA	Moc chłodnicza wymiennika ciepła minimum 25kW/szafę.
FUNKcjONALNOŚĆ KLIMATYZATORA	<p>Musi być wyposażony w system wentylatorów zapewniające odpowiedni wydatek powietrza poprzez możliwość regulacji prędkości obrotowej każdego wentylatora z osobna.</p> <p>Budowa modułu klimatyzatora musi zapewnić dostęp od przodu i tyłu w celach konserwacji i serwisu.</p> <p>Musi posiadać możliwość współpracy z modułem GSM umożliwiającym alternatywne powiadomienie o alarmach komunikatem SMS.</p> <p>Musi być wyposażony w moduł zarządzania i sterowania urządzeniem.</p> <p>Klimatyzator musi umożliwiać rejestrację parametrów pracy.</p> <p>Musi posiadać drzwi przednie i tylne w każdym wymienniku ciepła w celu łatwego dostępu serwisowego.</p> <p>System klimatyzacji musi posiadać protokół umożliwiający zarządzanie urządzeniem.</p> <p>W celu zapewnienia dostępu do danych procesowych przetwarzanych przez urządzenie musi posiadać zintegrowany serwer OPC.</p> <p>Możliwość obsługi funkcji Server Shutdown, automatycznego zamykania serwerów w zależności od występujących zdarzeń w ramach monitorowanych parametrów.</p> <p>Równoległa do SNMP możliwość komunikacyjna centralnego modułu monitorowania protokołem Modbus TCP IP.</p> <p>Możliwość wyboru trybu pracy wentylatorów – automatyczny lub manualny.</p> <p>Klimatyzator musi być wyposażony w złącze CAN-Bus dla łączenia magistrali czujników monitoringu parametrów fizycznych.</p> <p>Klimatyzator musi być wyposażony w czujniki temperatury oraz czujniki</p>

	<p>przepływu.</p> <p>Wymiana czujników temperatury wody musi być możliwa bez przerywania pracy urządzeń.</p> <p>Wymagane minimalne parametry monitorowania przez wymiennik ciepła pow/woda:</p> <ul style="list-style-type: none"> – pomiar obrotów wentylatorów wraz z alarmem w przypadku awarii, – pomiar temp. wody na wlocie, – pomiar temp. wody na wyjściu, – pomiar temp. powietrza na wlocie od przodu serwerów a także z tyłu serwerów na wylocie powietrza na każdym z trzech poziomów pionowych szafy,
AGREGAT CHŁODNICZY	<p>Dla układu klimatyzacji należy zaprojektować agregat schładzania wody wyposażony w zintegrowany system chłodzenia z odzyskiem energii.</p> <p>Moc chłodnicza agregatu minimum 48 kW.</p> <p>System chłodzenia z odzyskiem energii musi wykorzystywać temperaturę powietrza zewnętrznego do bezkosztowego schładzania wody w instalacji systemu klimatyzacji w przypadku gdy temperatura na powrocie do systemu jest o minimum 2°C niższa od temperatury powietrza zewnętrznego, zastępując chłodzenie realizowane przez sprężarki.</p> <p>Do projektowanego układu hydraulicznego należy przyjąć jeden czynnik chłodniczy w obiegu jako woda lodowa (woda z domieszką glikolu) a także agregat z redundancją w chłodzeniu w obiegu czynnika chłodniczego.</p> <p>Musi być wyposażony w system umożliwiający zdalne zarządzanie.</p> <p>System musi umożliwiać sprawdzanie ilości gazów chłodzenia oraz wilgoci w obwodzie schładzania.</p> <p>System musi sygnalizować wystąpienie nieprawidłowego ciśnienia.</p> <p>Agregat schładzania wody musi być wyposażony:</p> <ul style="list-style-type: none"> – w urządzenie sterujące prędkością wentylatora; – redundantne pompy sterowane ze sterownika systemu; – sprężarki z wewnętrznym zabezpieczeniem termicznym grzałki elektrycznej korpusu; – wymienniki ciepła po stronie skraplacza i po stronie parowacza, wyposażony w grzałkę zapobiegającą zamarzaniu. – filtr osuszacza; – elektrozawory zabezpieczające parowacz i sprężarki po wyłączeniu kompresora; – zawór termostatyczny na wylocie parowacza, do regulacji przepływu gazu do parowacza w zależności od obciążenia termicznego w taki sposób, aby zapewnić odpowiedni stopień przegrzania gazu na wlocie; – wentylatory z zabezpieczeniem termomagnetycznym i mechanicznym; – wyłącznik wysokiego oraz niskiego ciśnienia chroniący kompresor przed pracą przy nieprawidłowym ciśnieniu; – zawór zabezpieczający chłodzenia likwidujący nadciśnienie przy wystąpieniu nieprawidłowej wartości ciśnienia; – wyłącznik przepływu kontrolujący prawidłową cyrkulację wody w systemie hydraulicznym oraz wymienniku ciepła. – zbiornik buforowy zintegrowany z agregatem;

	<ul style="list-style-type: none"> – zawór upustowy odpowietrzający system; – zawór bezpieczeństwa likwidujący nadciśnienie w przypadku nieprawidłowej wartości ciśnienia; – amperomierz i przepływomierz; – styki beznapięciowe dla alarmu ogólnego, pompy, obwodu czynnika chłodzącego, czujnika temperatury i czujnika ciśnienia wody; – czujnik przeciwwzamrozeniowy do zabezpieczenia parowacza; – czujnik na wlocie wody; – czujnik na wylocie wody; – system zasilania awaryjnego UPS umożliwiający podtrzymanie zasilania; – układ podgrzewania umożliwiający pracę w temperaturze otoczenia zewnętrznego w zakresie od -20 do +40°C oraz zastosowanie obniżonej mieszanki z glikolem; – klawiaturę sterującą; – w zestaw awaryjnego chłodzenia wodą z wodociągów wraz z automatyką sterującą; – wibroizolatory instalowane do konstrukcji wsporczej agregatu; – system monitoringu urządzenia udostępniający informacje dotyczące minimum: <ul style="list-style-type: none"> ○ poboru mocy, ○ poboru prądu.
--	---

1.5. System sygnalizacji i gaszenia pożaru

Nazwa komponentu	Wymagane minimalne
WYMAGANIA OGÓLNE	<p>Każda z szaf musi zostać wyposażona w system wczesnego wykrywania i gaszenia panelami gaśniczymi o wysokości montażowej max. 1U w układzie Master > Slave, dla każdego rzędu jeden panel gaśniczy nadrzędny i dwa panele podrzędne połączone w jeden system, zapewniający ochronę każdej szafy serwerowej/sieciowej.</p> <p>Każda z szaf musi zostać wyposażona w systemy rurek ssących z elementami mocującymi.</p> <p>Każdy panel gaśniczy musi być wyposażony w wyświetlacz tekstowy dla komunikatów statusowych oraz minimum dwie zintegrowane czujki pożaru umożliwiające detekcję pożaru.</p> <p>System musi być wyposażony w zasilacz oraz zintegrowany systemem zasilania awaryjnego zapewniającego nieprzerwaną pracę systemu w czasie minimum 4 h.</p> <p>System musi być wyposażony w zintegrowany zbiornik o objętości minimum 2,0 l.</p> <p>Rozprowadzanie środka gaśniczego musi być realizowane poprzez rozładowanie ciśnienia z naboju gazu nośnego.</p> <p>Rozwiązanie musi zapewniać automatyczne rozbrojenie systemu gaszenia w przypadku otwarcia drzwi przednich lub tylnych szaf serwerowni i zasilania awaryjnego UPS.</p>
ŚRODEK GAŚNICZY	Novec TM 1230 firmy 3M TM lub równoważny.

PRZYŁĄCZA	<p>Zaciski przyłączeniowe wyjścia przekaźnikowego minimum: Alarm wstępny, Pożar, Gaszenie, Awaria.</p> <p>Gniazdo do podłączenia czujników otwarcia drzwi szaf z automatycznym rozbrajaniem systemu gaszenia w przypadku otwarcia drzwi szaf.</p> <p>Minimum 2 gniazda do połączenia z systemem monitorowania nadrzędnego dla całości infrastruktury IT.</p> <p>2 złącza CAN-Bus do połączenia w sieć paneli gaśniczych.</p> <p>Złącze zewnętrznego czujnika poziomu i sterowania zewnętrznym zbiornikiem (aktywne tylko w systemie wczesnego wykrywania pożaru z aktywnym układem zasysania dymu).</p> <p>Gniazdo przycisku pożarowego.</p> <p>Gniazdo czujnika drzwiowego.</p> <p>Złącze zbiorcze umożliwiające przesyłanie komunikatów minimum: Uruchomienie zewnętrzne, Pożar, Awaria akumulatora, Awaria przepływu powietrza, Awaria czujki, Awaria komunikacji, Awaria wyjście gaszenia, Ubytek środka gaśniczego, Awaria przycisku pożarowego, System gaszenia zablokowany, Awaria zasilacza.</p>
CZUJNIKI	<p>Główny panel gaśniczy o wysokości 1U musi być wyposażony w:</p> <ul style="list-style-type: none"> – minimum 2 osobne czujniki światła rozproszonego dla 2 progów alarmu, – optyczną czujkę dymu (czułość ok. 3,5%/m zmętnienia światła); – optyczną czujkę dymu o wysokiej czułości (czułość ok. 0,25 %/m zmętnienia światła)

1.6. Systemu monitoringu wizyjnego

Nazwa komponentu	Wymagane minimalne
WYMAGANIA OGÓLNE	<p>Do obserwacji pomieszczeń serwerowni GCPD oraz ZCPD oraz otoczenia bezpośrednio przed nimi, w celu poprawy stanu bezpieczeństwa urządzeń teleinformatycznych, zainstalowanych w serwerowni, Zamawiający wymaga dostarczenia, konfiguracji i instalacji system rejestracji obrazu składającego się z:</p> <ul style="list-style-type: none"> – 10 kopułkowych kamer IP, w obudowie metalowej IP67, o minimalnej rozdzielczości 2688x1520, pracujących w trybie Dzień/Noc. Budowa kamer musi umożliwiać montaż sufitowy lub naścienny; – rejestratora sieciowego do zapisu obrazu, przystosowanego do montażu w szafach typu RACK, wyposażonego w dyski do zapisu ciągłego (NVR). <p>Zamawiający wymaga wykonania całości okablowania do transmisji sygnałów wizyjnych. Miejsca instalacji kamer zostaną określone przez Zamawiającego na etapie realizacji zadania.</p>
KAMERA	<p>Przetwornik - CMOS 1/3";</p> <p>Obiektyw - ogniskowa 2,7 mm – 13,5 mm, wyposażony w motozoom;</p> <p>Kompresja wideo – H.265;</p> <p>Obsługiwane protokoły - HTTP, TCP, RTSP, RTP, UDP, RTCP, SMTP, FTP,</p>

	<p>DHCP, DNS, DDNS, IPv4/v6, SNMP, UPnP, NTP;</p> <p>Kąt widzenia - 104° - 28°</p> <p>Musi być wyposażona w doświetlacz IR, z zasięgiem podczerwieni minimum 30 m.</p> <p>Musi zapewniać obsługę kart pamięci.</p> <p>Musi umożliwiać wykrywanie ruchu.</p>
REJESTRATOR	<p>Musi być wyposażony w procesor wielordzeniowy – minimum 4 rdzenie.</p> <p>Musi umożliwiać obsługę minimum 128 kanałów IP w rozdzielczości 12MPX.</p> <p>Musi być wyposażony w co najmniej jedno wejście oraz jedno wyjście audio RCA.</p> <p>Musi posiadać dwa wyjścia HDMI w standardzie 2.0, umożliwiające obsługę rozdzielczości 3840 x 2160. Oba wyjścia powinny działać niezależnie.</p> <p>Wyjścia graficzne muszą obsługiwać następujące rozdzielczości: 3840 x 2160 , 1920 x 1080 , 1280 x 1024, 1280 x 720 , 1024 x 768.</p> <p>Musi umożliwiać tworzenie podziałów do 36 kamer na jednym ekranie. Ponadto, musi umożliwiać definiowanie widoków własnych, jak i rysowanie swoich własnych podziałów, np. składających się z jednej kamery panoramicznej obejmującej całą szerokość wyświetlacza.</p> <p>Musi obsługiwać kodowanie H.264 jak i H.265.</p> <p>Wydajność zapisu – minimum 384Mbps.</p> <p>Musi obsługiwać co najmniej 3 strumienie z kamer. Wyświetlanie strumienia głównego musi być realizowane w pełnej rozdzielczości, z możliwością automatycznego przełączanie na strumień pomocniczy przy podziałach 3x3 i wyższych oraz jednoczesny zapis strumienia trzeciego.</p> <p>Musi umożliwiać współpracę z kamerami w standardzie ONVIF jak również przyjmować strumienie RTSP.</p> <p>Musi posiadać przynajmniej 4 niezależne porty sieciowe o przepustowości 1000 Mbps oraz 2 interfejsy światłowodowe. Porty powinny umożliwiać pracę w trybie niezależnych interfejsów lub redundancji, lub trybu load-balancing.</p> <p>Musi mieć zainstalowane minimum 16 dysków twardych o pojemności min. 8TB każdy.</p> <p>Musi umożliwiać obsługę RAID minimum na poziomie 0/1/5/10.</p> <p>Dostępne porty: 2x USB2.0, 2x USB3.0 RS232 1 Port, dla komunikacji z PC oraz klawiaturą RS485 1 Port, dla obsługi PTZ.</p> <p>Zasilacze redundantne.</p>
OPROGRAMOWANIE	<p>Musi być dostarczony wraz z oprogramowaniem pozwalającym na centralne konfigurowanie, zarządzanie, monitorowanie wszystkimi kamerami oraz rejestratorem.</p>
MONITORY	<p>Zamawiający wymaga dostarczenia dwóch monitorów/telewizorów o parametrach:</p> <p>Ekran min. 40 cale, o rozdzielczości min. 1920 x 1080</p> <p>Funkcje Wi-Fi, min. 2x HDMI, min. 1x USB</p>

1.7. Systemu kontroli dostępu.

Nazwa komponentu	Wymagane minimalne
Wymagania ogólne	<p>Dla potrzeb GCPD oraz ZCPD, zamawiający wymaga dostawy i instalacji systemu kontroli dostępu wyposażonego w 14 czytników typu MIFARE 13.56 MHz, umożliwiających odczyt kart z odległości minimum 2 cm</p> <p>System kontroli dostępu musi rejestrować wejścia do pomieszczenia serwerowni, bazując na identyfikacji użytkowników za pomocą kodów PIN oraz kart zbliżeniowych.</p> <p>System musi składać się z kontrolera dostępu, zasilacza i akumulatora umożliwiającego podtrzymanie zasilania po zaniku zasilania sieci głównej, zamkniętych w jednej obudowie metalowej oraz czytnika zbliżeniowego z klawiaturą numeryczną.</p> <p>Musi mieć możliwość zdefiniowania minimum 6 grup dostępu.</p> <p>Musi być wyposażony w pamięć pozwalających na zapis minimum 100.000 zdarzeń.</p>
Komunikacja	Ethernet TCP/IP, RS-485, Wiegand
Oprogramowanie	Musi być dostarczony wraz z oprogramowaniem pozwalającym na centralne zarządzanie wszystkimi czytnikami.

2. Zapasowe Centrum Przetwarzania Danych

2.1. Wymagania ogólne

Dla potrzeb Zapasowego Centrum Przetwarzania Danych (ZCPD), Zamawiający wymaga dostawy wraz z montażem i uruchomieniem modułowego systemu szaf szczelnych zintegrowanych z systemem klimatyzacji precyzyjnej w oparciu o instalację DX z bezpośrednim odparowaniem zapewniającym odbiór zysków ciepła poprzez między szafowe jednostki chłodnicze, pracujące w układzie szczelnym oraz skraplacze zdalne, składający się z minimum:

- 2 szaf serwerowych typu RACK 19" o wymiarach 600x1200x42U,
- 1 szafy na infrastrukturę LAN typu RACK 19" o wymiarach 800x1200x42U,
- zintegrowanego systemu klimatyzacji międzyszafowej ,
- zintegrowanego systemu sygnalizacji i gaszenia pożaru,

oraz wykonania koniecznych prac adaptacyjnych pomieszczenia serwerowni, obejmujące:

- montaż drzwi wejściowych antywłamaniowych, o podwyższonej odporności ogniowej;
- demontaż instalacji centralnego ogrzewania;
- malowanie ścian i wykonanie zabezpieczeń ognioochronne w klasie odporności ogniowej 60 minut. Zabezpieczenie dotyczy ścian, stropów, przepustów;

Przed montażem w/w urządzeń Zamawiający wymaga wykonanie projektu instalacji elektrycznej obejmującej przyłącze elektryczne serwerowni oraz instalacji systemu chłodzenia opartego, w którym czynnikiem chłodzącym będzie czynnik R410A.

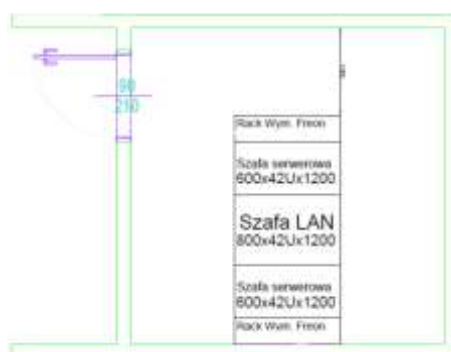
Projekt wykonawczy musi zawierać co najmniej:

- Opis rozwiązania,

- Rysunki (plany) lokalizacji głównych elementów instalacji, prowadzenie instalacji, rysunki elementów systemu, rysunki przyłącza agregatu, schematy blokowe – potrzebne wykonawcy do realizacji zadania,
- Sposób wykonania pomiarów - w projekcie wykonawczym należy zawrzeć warunek wykonania pomiarów torów transmisyjnych zgodnie z obowiązującą specyfikacją Kat.6,
- Specyfikację materiałową,
- Specyfikację techniczną budowy i odbioru robót,
- Informację dotyczącą bezpieczeństwa i ochrony zdrowia

Ze względu na ograniczenia powierzchni ZCPD, moduły należy montować w układzie jednorzędowym. Ilość i rozmieszczenie modułów systemu klimatyzacji musi zapewnić optymalne warunki chłodzenia dla wszystkich szaf systemu.

Ze względu na ograniczenia powierzchni ZCPD, moduły należy montować w układzie jednorzędowym zgodnie przykładowym schematem rozmieszczenia szaf.



Zamawiający dopuszcza zmianę układu rozmieszczenia szaf w rzędzie oraz ilości i układu wymienników ciepła w celu zapewnienia optymalnych warunków chłodzenia oferowanego rozwiązania pod warunkiem wcześniejszej konsultacji i akceptacji przez Zamawiającego.

System szaf szczelnych klimatyzowanych musi być dostarczony wraz z systemem zarządzania infrastrukturą serwerowni i monitorowania warunków fizycznych.

2.2. Dostosowanie pomieszczenia

W ramach prac przygotowujących pomieszczenie do funkcji serwerowni należy ściany przylegające do pomieszczeń służbowych zabezpieczyć min. 5cm warstwą dźwiękoszczelną o klasie odporności ogniowej min. 60 minut, jedna ściana – powierzchnia do zabezpieczenia to max. 15 m².

Wszystkie ściany należy zabezpieczyć aby uzyskać odporność ogniową 60 minut np. odpowiednimi płytami karton gips. – powierzchnia do wykonania max. 50m².

Ściany oraz sufit należy pomalować przynajmniej dwukrotnie farbą o takiej samej klasie odporności ogniowej – powierzchnia do malowania to max. 70m².

Przepusty istniejące i nowe również należy zabezpieczyć klasą odporności ogniowej 60 minut.

Strop powinien spełniać normę odporności ogniowej 60 minut, w tym, celu należy zweryfikować czy konieczne jest dodatkowe zabezpieczenie i odpowiednio zabezpieczyć jeżeli jest to konieczne – powierzchnia max. 20m².

Podłogę należy pokryć wykładziną elektrostatyczną – powierzchnia max. 20 m².

2.3. Drzwi wejściowe antywłamaniowe o podwyższonej odporności ogniowej

Zamawiający wymaga dostarczenia wraz z montażem stalowych drzwi antywłamaniowych spełniających warunki normy PN-EN 1627:2011 o odporności ogniowej EI60, o wymiarach co najmniej 100 cm szerokość na 210 cm wysokość. Drzwi muszą być wyposażone w 2 zamki atestowane w klasie C oraz muszą posiadać tabliczkę znamionową zawierającą potwierdzenie posiadania Certyfikatu Instytutu Mechaniki Precyzyjnej lub Instytutu Techniki Budowlanej.

Drzwi muszą być wyposażone w rygiel elektromagnetyczny rewersyjny, niskoprądowy lub zwoję elektromagnetyczną. Na ścianie wewnątrz pomieszczenia należy umieścić wyłącznik ewakuacyjny.

Drzwi mają współpracować z systemem kontroli dostępu do pomieszczeń.

2.4. Zabezpieczenia okien

W ramach prac adaptacyjnych należy zabezpieczyć okna Zapasowego Centrum Przetwarzania danych poprzez montaż stalowych krat antywłamaniowych malowanych proszkowo w kolorze RAL. Szybę okna po wewnętrznej stronie należy pokryć folią utrudniającą włamanie i rozbicie, spełniającą wymogi klasy antywłamaniowej P2A-ITB "odporność na ręczny atak".

W celu redukcji nasłonecznienia na zewnętrznej stronie szyby należy nakleić folię, która posiada metalizowaną lub napyłaną warstwę odbijającą energię słoneczną.

Zamawiający dopuszcza również rozwiązanie polegające na zamurowaniu otworu okiennego przy zachowaniu wszystkich wymagań projektowych, bezpieczeństwa, zezwoleń niezbędnych do realizacji takiego rozwiązania.

2.5. Instalacje elektryczne

W ramach realizacji zamówienia w Zapasowym Centrum Przetwarzania Danych należy wykonać:

- 1) dedykowane przyłącze elektryczne dla potrzeb zasilania modułowego systemu szaf zintegrowanych z systemem klimatyzacji i urządzeń serwerowych;
- 2) instalacje elektryczne w zakresie oświetlenia podstawowego – dwie lampy o strumień światła wynoszący min. 400lm, odporności ogniowej min. 60 minut - awaryjnego – jedna lampa z podtrzymaniem 3h, strumieniu światła 300lm i odporności ogniowej min. 60 minut, oświetlenia ewakuacyjnego, zasilania ogólnego;

Zamawiający wymaga dla w/w instalacji wykonanie dokumentacji projektowej uwzględniającej szczegółowo zakres i specyfikę prac instalacyjnych. Dokumentacja projektowa musi składać się z Projektu Wykonawczego, Specyfikacji Technicznej Wykonania i Odbioru Robót oraz zawierać informację dotyczącą bezpieczeństwa i ochrony zdrowia.

Projekty elektryczne powinny być wykonane i sprawdzone przez osoby posiadające uprawnienia budowlane bez ograniczeń w branży teleinformatycznej elektrycznej oraz posiadające aktualne zaświadczenie Okręgowej Izby Inżynierów. Projekty sieci

teleinformatycznej muszą być wykonane i sprawdzone przez uprawnionego projektanta wybranego systemu okablowania strukturalnego, oraz posiadające aktualne zaświadczenie o wydanych uprawnieniach projektowych.

Dedykowane przyłącze elektryczne dla potrzeb zasilania urządzeń serwerowych

W pomieszczeniu serwerowni należy wykonać tablicę rozdzielczą wyposażoną w odpowiednią ilość wyłączników różnicowo-prądowych (min. 3) i nadprądowych. Tablicę należy uziemić zgodnie z przepisami szczegółowymi dla tego typu obiektów oraz z normami Prawa Budowlanego. Do rozdzielni, należy doprowadzić niezależne linie zasilające (WLZ), poprowadzone z rozdzielni – max odległość 200m z rozdzielni.

Przekrój kabla linii WZL musi zapewnić możliwość podpięcia 3 szaf serwerowych, UPS-ów przewidzianych do podtrzymywania urządzeń zainstalowanych w szafach, systemu klimatyzacji precyzyjnej oraz oświetlenia. Do celów projektowych należy przyjąć maksymalne obciążenie jednej szafy wynoszące 10kVA.

Należy wykonać instalację uziemiającą dla modułowego systemu szaf RACK zintegrowanych z system klimatyzacji precyzyjnej.

2.6. Wykonanie instalacji i konfiguracji systemów bezpieczeństwa

W ramach przygotowywania pomieszczenia Zapasowego Centrum Przetwarzania Danych należy wykonać instalację, konfigurację systemu kontroli dostępu do pomieszczeń. Jeżeli pomieszczenia będzie wymagało dostosowania – okablowanie sieci LAN, zasilanie, uchwyty itp. – Wykonawca powinien to uwzględnić w swojej ofercie. Oferta powinna zawierać także wycenę prac instalacji i konfiguracji systemu monitoringu również uwzględniającą konieczne elementy – okablowanie, uchwyty, zasilanie – do realizacji tej usługi.

System bezpieczeństwa – system kontroli dostępu, system monitoringu – po realizacji usługi instalacji i konfiguracji musi w celu odbioru prac realizować wszystkie wymagane od systemów funkcje oraz być zintegrowany z systemem zainstalowanym w Głównym Centrum Przetwarzania Danych.

2.7. Szafy RACK 19" 42U

Nazwa komponentu	Wymagane minimalne
WYMAGANIA OGÓLNE	<p>Stelaż szaf musi być wykonany ze spawanej ramy odpornej na skręcanie, o nośności minimum 1500 kg.</p> <p>Płaskość montażowa 19" musi składać się z uniwersalnych szyn profilowych do zastosowań serwerowych, sieciowych i elektronicznych.</p> <p>Szyny profilowe z tyłu muszą być przygotowane do obustronnego zamocowania list zasilających PDU (Power Distribution Unit) w przestrzeni 0 U.</p> <p>Elementy szafy wykonane z blachy stalowej lub aluminium, malowane proszkowo w kolorze RAL.</p> <p>Szafy muszą być szczelne, przystosowane do systemów chłodzenia wewnętrznego (w obrysie szafy).</p>
DRZWI	<p>Przednie drzwi przeszklone z szybą wykonaną ze szkła hartowanego o szczelności na poziomie IP54, wyposażone w zamek dźwigienkowy.</p>

	<p>Drzwi muszą być wyposażone w systemową kontrolę dostępu, zapewniającą współpracę z zastosowanymi wymiennikami ciepła powietrze woda oraz muszą współpracować z systemem automatycznego awaryjnego otwarcia drzwi szaf.</p> <p>Tylne drzwi pełne z blachy stalowej, zamykane na zamek.</p>
PŁYTA DACHOWA	<p>Możliwość bocznego wprowadzania kabli przez listwy szczotkowe.</p> <p>Możliwość instalacji wentylatorów.</p>
PŁYTA PODŁOGOWA	<p>Płyta podłogowa przygotowana na przepusty piankowe pozwalająca na wprowadzenie kabli przy zachowaniu zakładanej szczelności szafy.</p> <p>Wszystkie skręcone części poszycia podłogi z automatycznym wyrównaniem potencjałów i przygotowaniem do mocowania taśm uziemienia.</p>
WYPOSAŻENIE PODSTAWOWE	<p>Każda szafa serwerowa musi być wyposażona w minimum:</p> <ul style="list-style-type: none"> – 8 stalowych ocynkowanych lub malowanych proszkowo szyn montażowych poziomych, montowane po głębokości szaf 1200mm po 4 szt. na lewą i prawą stronę; – 10 szt. kablowych wieszaków przelotowych do elastycznego i uporządkowanego prowadzenia okablowania, bocznie na szynach profilowych; – boczny kanał kablowy pozwalający na prowadzenie okablowania w pionie oraz przeprowadzenie kabli do wnętrza szafy; – 3 szt. 19" paneli zaślepiających 3U. Panele zaślepiające mają zapewnić odpowiednie prowadzenie powietrza oraz zapewnić właściwy sposób rozprowadzenia gazu gaśniczego. Każdy panel musi posiadać odporność ogniową według standardu UL 94 HB lub równoważnego i musi być samogasnący;
LISTWY ZASILAJĄCE PDU	<p>Szafy serwerowe oraz na infrastrukturę LAN muszą posiadać po minimum dwie pionowe listwy zasilające PDU 400V 50/60 Hz, opomiarowane na każdą z faz z podłączeniem do sieci zdalnego monitorowania.</p> <p>Listwy PDU muszą posiadać możliwość montażu w przestrzeni pomiędzy ścianą boczną a profilem 19" w dedykowanych zatokach szafy przeznaczonych na dystrybucję zasilania oraz alternatywnie po dwie bliźniaczo, na stronę lewą lub prawą.</p> <p>Minimalna ilość i typ gniazd EN 60320: 18 x C13, 4 x C19.</p> <p>Funkcje pomiarowe: Napięcie (V) w zakresie 90V-250V, prąd (A) w zakresie 0,1A-16A, częstotliwość (Hz), Moc czynna (kW), praca czynna (kWh), moc bierna, Współczynnik mocy (cos Ø), moc pozorna (VA).</p> <p>Możliwość zdalnego monitorowania z wykorzystaniem protokołów http, HTTPS, SSL, SSH oraz usługi Telnet.</p> <p>Obsługiwane protokoły komunikacyjne: TCP/IP, SNMP, FTP/SFTP.</p> <p>Możliwość podłączenia do każdego PDU czujników monitoringu: czujnik temperatury, czujnik temperatury / wilgotności.</p>
MONITORING WARUNKÓW ŚRODOWISKOWYCH	<p>Szafy muszą być wyposażone w system monitoringu infrastruktury fizycznej pozwalający na:</p> <ul style="list-style-type: none"> – pomiar temperatury w szczelnie zamkniętych szafach w zakresie 10°C – 50°C;

	<p>– pomiar wilgotności w szczelnie zamkniętych szafach w zakresie 10% - 95%.</p> <p>System monitoringu musi być dostarczony z czujnikami umożliwiającymi pomiar temperatury i wilgotności oraz czujnik wykrywający wyciek w pomieszczeniu serwerowni. Wymagane są podziały wykrycia wycieku na strefy od 1 do 5 na długości max. 15m.</p> <p>System musi umożliwiać monitorowanie parametrów fizycznych wyodrębnionych elementów całościowego systemu infrastruktury IT za pomocą protokołu CAN-Bus: listew dystrybucji zasilania PDU, systemu wczesnego wykrywania i gaszenia pożaru w szafach zamkniętych, klimatyzacji międzyszafowej opartej na systemie schładzanej wody z glikolem, agregatów chłodzenia cieczy IT, systemu szaf zasilania awaryjnego UPS.</p> <p>System musi umożliwiać zdalny monitoring paneli gaśniczych 19”.</p> <p>System musi umożliwiać zdalny monitoring i sterowanie dla automatycznego awaryjnego otwarcia drzwi szaf.</p> <p>Musi umożliwiać monitoring i zarządzanie zdalne listwami dystrybucji energii PDU.</p> <p>Obsługiwane protokoły: TCP/IP, SNMPv1, SNMPv2c, SNMPv3, SSH, FTP, SFTP, HTTP, HTTPS, NTP, DHCP, DNS, SMTP, XML*, Syslog.</p> <p>Musi umożliwiać równoległą do SNMP możliwość komunikacji z centralnym modułem monitorowania za pomocą protokołu Modbus TCP IP.</p> <p>System musi być wyposażony w zegar czasu rzeczywistego z NT.</p> <p>System musi umożliwiać zdalną kontrolę i zarządzania.</p> <p>System musi umożliwiać współpracę z przewidzianym modułem GSM 4G pozwalającym na alternatywne powiadomienia alarmowe, ostrzeżenia komunikatem SMS.</p>
INNE	Każda szafa musi być wyposażona w system automatycznego awaryjnego otwarcia drzwi.

2.8. System zasilania awaryjnego UPS

Nazwa komponentu	Wymagane minimalne
WYMAGANIA OGÓLNE	<p>W celu ochrony przed zakłóceniami i nieregularnościami publicznej sieci zasilania wrażliwych na napięcie odbiorników, ma być zastosowany statyczny system zasilania bezprzerwowego (UPS).</p> <p>Ma być zbudowany jako system z redundancją n+1, składający się z 2 szt. połączonych równolegle modułów 20 kW.</p> <p>Aby ułatwić obsługę, moduły UPS muszą być wykonane w technice wsuwanej i wbudowane w 19” ramy systemowe.</p> <p>Każdy moduł musi być całkowicie zamknięty w metalowej obudowie umożliwiającej odseparowanie go od pozostałych modułów.</p> <p>Niezależnie od mocy potrzebnej w rozbudowie końcowej, musi mieć</p>

	<p>możliwość indywidualnego dopasowania do odbiorników i rozbudowy wraz ze wzrostem zapotrzebowania na moc.</p> <p>Każdy z połączonych równolegle modułów UPS musi być całkowicie autonomiczny oraz musi posiadać własny system sterowania i obejścia (przełącznik obejściowy).</p> <p>Każdy moduł musi składać się z części funkcjonalnych: prostownika, boostera, falownika, obwodu baterii, przetwornika DC do ładowania akumulatorów bez falowania, jednostki wyświetlacza i elektronicznego obejścia.</p> <p>Ramy systemowe muszą umożliwiać zainstalowanie minimum 2 moduły UPS na ramę. Rama musi dać się zintegrować ze standardowym stelażem 19”.</p> <p>Rama musi posiadać złącza zaciskowe wejściowe i wyjściowe oraz obejście ręczne (przełącznik serwisowy).</p> <p>Wymiana uszkodzonego modułu UPS, ze względów dostępności, musi być możliwa bez przerywania pracy i bez przełączania na elektroniczne obejście serwisowe do niezabezpieczonej sieci.</p> <p>W celu osiągnięcia maksymalnego możliwego bezpieczeństwa zasilania dla podłączonych odbiorników, dopuszczalne są tylko systemy działające zgodnie z zasadą trybu online wg klasyfikacji VFI-SS-111 (voltage and frequency independent) wg EN 62040-3 lub równoważnej.</p> <p>System UPS musi dysponować automatycznym testem baterii, uruchamianym regularnie w dowolnie zaprogramowanych odstępach czasu.</p>
MOC ZNAMIONOWA	20 kV / 20 kW każdy moduł bateryjny
WEJŚCIE	<p>Napięcie: 3 x 400/230 V</p> <p>Częstotliwość sieciowa: 50 Hz</p> <p>Zakres częstotliwości bez rozładowania baterii: 40 - 70 Hz</p> <p>THDI: < 3%</p> <p>Współczynnik mocy wejściowej: $\geq 0,99$</p>
WYJŚCIE	<p>Napięcie: 400/230V</p> <p>Częstotliwość: 50Hz</p> <p>Przeciążalność: minimum 125%/10min</p> <p>Sprawność przy obciążeniu liniowym >75%: $\geq 95\%$</p>
TYO BATERII	VRLA lub równoważny
CZAS PODTRZYMANIA BATERYJNEGO	minimum 10 minut
INNE	<p>Osobne zasilanie dla obejścia i prostownika.</p> <p>Złącza: RS-232, USB.</p> <p>Oprogramowanie do zarządzania urządzeniem.</p>

2.9. System klimatyzacji

Nazwa komponentu	Wymagane minimalne
WYMAGANIA OGÓLNE	<p>System klimatyzacji musi zapewnić chłodzenie wszystkich dostarczonych szaf przy uwzględnieniu ich nominalnego wyposażenia i obciążenia cieplnego.</p> <p>W celu zapewnienia optymalnego chłodzenia urządzeń dla szczelnie zamkniętych szaf należy zaprojektować minimum dwa klimatyzatory międzyrzędowe bezpośrednie odparowanie zintegrowane z szafami serwerowymi.</p> <p>Musi współpracować ze skraplaczem zamontowanym na zewnątrz budynku.</p> <p>Temperatura pracy skraplaczy zewnętrznych: do minimum -40°C</p> <p>Instalację zasilającą oraz powrót czynnika chłodniczego należy zlokalizować po podłogą techniczną.</p> <p>Prowadzenie powietrza musi opierać się na zasadzie chłodzenia wbudowanych w szafie urządzeń "front to back".</p> <p>Regulacja temperatury wdmuchiwanego zimnego powietrza musi odbywać się poprzez stałe wyrównanie temperatury rzeczywistej z temperaturą zadaną na wymienniku ciepła.</p> <p>Klimatyzator i zewnętrzny skraplacz muszą być połączone odpowiednim miedzianym przewodem rurowym wg PN-EN 378-2.</p> <p>Podłączenie urządzeń chłodniczych, wymienników do przewodów czynnika chłodniczego oraz przyłącza elektryczne muszą dawać możliwość wykonania podłączenia od dołu lub od góry szaf.</p> <p>Urządzenia chłodnicze muszą być wyposażone w zarządzanie kondensatem zbierającym się w kolektorze i stamtąd odprowadzane do instalacji kanalizacyjnej.</p>
CZYNNIK CHŁODNICZY	R410A lub równoważny
MOC KLIMATYZATORA	Moc chłodnicza wymiennika ciepła minimum 12kW/szafę.
FUNKCJONALNOŚĆ KLIMATYZATORA	<p>Musi być wyposażony w wentylatory redundantne $n + 1$ z zasilaniem 3-fazowym – w przypadku braku jednej fazy zasilania elektrycznego system musi zapewnić dalsze działanie systemu.</p> <p>Wymiennik musi być wyposażony w minimum 4 wentylatory typu EC.</p> <p>Wymiennik musi zasysać ciepłe powietrze wylotowe z serwera z tyłu szafy RACK, a schłodzone powietrze dostarczać w przednią część szafy RACK.</p> <p>Budowa modułu klimatyzatora musi zapewnić dostęp od przodu i tyłu w celach konserwacji i serwisu.</p> <p>Wymiennik musi posiadać zintegrowaną sprężarkę inwerterową wraz z dedykowanym sterownikiem regulującym obroty.</p> <p>Musi posiadać możliwość współpracy z modułem GSM umożliwiającym alternatywne powiadomienie o alarmach komunikatem SMS.</p>

	<p>Musi być wyposażony w moduł zarządzania i sterowania urządzeniem.</p> <p>Musi posiadać drzwi przednie i tylne w każdym wymienniku ciepła w celu łatwego dostępu serwisowego.</p> <p>Możliwość obsługi funkcji Server Shutdown, automatycznego zamykania serwerów w zależności od występujących zdarzeń w ramach monitorowanych parametrów.</p> <p>Równoległa do SNMP możliwość komunikacyjna centralnego modułu monitorowania protokołem Modbus TCP IP.</p> <p>Drzwi przednie i tylne muszą być wyposażone w czujniki monitorujące ich otwarcie oraz rozbrojenie zintegrowanego w szafach systemu gaszenia.</p>
--	--

2.10. System sygnalizacji i gaszenia pożaru.

Nazwa komponentu	Wymagane minimalne
WYMAGANIA OGÓLNE	<p>Każda z szaf musi zostać wyposażona w system wczesnego wykrywania i gaszenia panelami gaśniczymi o wysokości montażowej max. 1U w układzie Master > Slave, dla każdego rzędu jeden panel gaśniczy nadrzędny i dwa panele podrzędne połączone w jeden system, zapewniający ochronę każdej szafy serwerowej/sieciowej.</p> <p>Każda z szaf musi zostać wyposażona w systemy rurek ssących z elementami mocującymi.</p> <p>Każdy panel gaśniczy musi być wyposażony w wyświetlacz tekstowy dla komunikatów statusowych oraz minimum dwie zintegrowane czujki pożaru umożliwiające detekcję pożaru.</p> <p>System musi być wyposażony w zasilacz oraz zintegrowany systemem zasilania awaryjnego zapewniającego nieprzerwaną pracę systemu w czasie minimum 4 h.</p> <p>System musi być wyposażony w zintegrowany zbiornik o objętości 2,0 l.</p> <p>Rozprowadzanie środka gaśniczego musi być realizowane poprzez rozładowanie ciśnienia z naboju gazu nośnego.</p> <p>Rozwiązanie musi zapewniać automatyczne rozbrojenie systemu gaszenia w przypadku otwarcia drzwi przednich lub tylnych szaf serwerowni i zasilania awaryjnego UPS.</p>
ŚRODEK GAŚNICZY	Novec™ 1230 firmy 3M™ lub równoważny.
PRZYŁĄCZA	<p>Zaciski przyłączeniowe wyjścia przekaźnikowego minimum: Alarm wstępny, Pożar, Gaszenie, Awaria.</p> <p>Minimum 2 gniazda do połączenia z systemem monitorowania nadrzędnego dla całości infrastruktury IT.</p> <p>2 złącza CAN-Bus do połączenia w sieć paneli gaśniczych.</p> <p>Złącze zewnętrznego czujnika poziomu i sterowania zewnętrznym zbiornikiem (aktywne tylko w systemie wczesnego wykrywania pożaru z aktywnym układem zasysania dymu).</p> <p>Gniazdo przycisku pożarowego.</p> <p>Gniazdo czujnika drzwiowego.</p> <p>Złącze zbiorcze umożliwiające przesyłanie komunikatów minimum:</p>

	Uruchomienie zewnętrzne, Pożar, Awaria akumulatora, Awaria przepływu powietrza, Awaria czujki, Awaria komunikacji, Awaria wyjście gaszenia, Ubytek środka gaśniczego, Awaria przycisku pożarowego, System gaszenia zablokowany, Awaria zasilacza.
CZUJNIKI	Moduł główny gaszenia musi być wyposażony w: – minimum 2 osobne czujniki światła rozproszonego dla 2 progów alarmu, – optyczną czujkę dymu.

2.11. System monitoringu wizyjnego.

Zgodnie z pkt 1.6.

2.12. System kontroli dostępu.

Zgodnie z pkt 1.7.

3. Światłowodowa sieć LAN

3.1. Okablowanie

Sieć LAN GCPD należy połączyć z infrastrukturą teletechniczną ZCPD za pomocą zewnętrznego kabla światłowodowego 24x9/125, włókno G652D w powłoce PE.

Kabel pomiędzy budynkami będzie ułożony i prowadzony w istniejących lub powstających w ramach odrębnej inwestycji kanałach kablowych. Długość łącza światłowodowego około 500 m.

Szafy serwerowe należy wyposażać w przełącznice światłowodowe 19" z wysuwaną szufladą, w których zostaną zakończone włókna światłowodowe. Przełącznica musi zawierać minimum 2 kasety na spawy, pigtaile oraz adaptory SC/APC.

Panele krosowe światłowodowe muszą być zamontowane w szafie dystrybucyjnej na stelażu 19" za pomocą zestawu elementów śrub mocujących (4x śruba, podkładka oraz nakrętka). Instalacja winna przebiegać zgodnie z kartą katalogową danego urządzenia.

Każda końcówka kabla światłowodowego powinna być wprowadzona do obudowy (panela krosowego, puszki instalacyjnej z elementem zapasu włókien) stanowiącej ochronę włókien światłowodowych oraz miejsce, w którym należy przygotować odpowiedni zapas włókien: w panelach światłowodowych – ok. 2 m, w puszkach instalacyjnych – od 0,5 do 1m.

Po wykonaniu połączeń należy przeprowadzić pomiary reflektometryczne dwukierunkowo za pomocą analizatora posiadającego aktualny certyfikat potwierdzający jego dokładność. Pomiar powinien zawierać:

- Specyfikację (normę) wg której jest wykonywany pomiar
- Metodę referencji
- Tłumienie toru pomiarowego
- Podane wartości graniczne (limit)
- Podane zapasy (najgorszy przypadek)
- Informację o końcowym rezultacie pomiaru

Na raportach pomiarów powinna znaleźć się informacja opisująca wysokość marginesu pracy (inaczej zapasu lub marginesu bezpieczeństwa, tj. różnicy pomiędzy wymaganiem normy a pomiarem, zazwyczaj wyrażana w jednostkach odpowiednich dla każdej wielkości mierzonej) podanych przy najgorszych przypadkach. Parametry transmisyjne muszą być poddane analizie w całej wymaganej dziedzinie częstotliwości/tłumienia. Zapasy (margines bezpieczeństwa) musi być podany na raporcie pomiarowym dla każdego oddzielnego toru światłowodowego.

W ramach realizacji zadania należy dostarczyć, zainstalować zgodnie z wytycznymi Zamawiającego na etapie realizacji oraz skonfigurować urządzenia sieciowe:

- przełącznik szkieletowy 48 portowy SFP+ - 2 szt.
- przełącznik brzegowy 48 portowy Base-T - 2 szt.
- oprogramowanie do zarządzania urządzeniami sieci
- urządzenie brzegowe klasy UTM - 1 szt.

3.2. Urządzenia sieciowe

1) Przełącznik szkieletowy 48 portowy SFP+

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Obudowa typu RACK 19"; Wysokość maksymalna 1U; Musi posiadać minimum 2 wymienne moduły zasilacza AC (hot-swap);
Pamięć	Wbudowana pamięć RAM min. 4GB; Pojemność bufora pakietów: 20MB;
Porty	Minimum 48 x 10 Gigabit Ethernet SFP+ Minimum 6 x 100 Gigabit Ethernet QSFP28 Minimum 1 port konsolowy RJ45 Minimum 1 port ethernet RJ-45, out-of-band management Minimum 1 port -USB
Wydajność	Musi posiadać matrycę przełączającą o wydajności min. 2Tbps (full-duplex), Wydajność przełączania przynajmniej 450Mpps; Musi obsługiwać ramki „Jumbo” o długości min. 9000 B; Obsługa min. 160 000 adresów MAC; Obsługa min. 4000 sieci VLAN jednocześnie; Rozmiar tablicy ARP minimum: 128 000; Musi obsługiwać, co najmniej protokoły: STP, RSTP, PVST+ lub VBST, MSTP (minimum 64 instancje); Musi wspierać funkcjonalność wirtualnej agregacji portów umożliwiającą: - terminowanie pojedynczej wiązki EtherChannel/LACP ; Urządzenie musi posiadać możliwość definiowania łączy w grupy LAG (802.3ad). Obsługa min. 16 łączy w grupie LAG; Musi obsługiwać DCB (Data Center Bridging), 802.1Qbb Priority-Based Flow

	Control, funkcjonalność DCB oraz PFC;
Routing	<p>Musi obsługiwać protokoły dynamicznego routing dla IPv4 i dla IPv6: OSPF, BGP</p> <p>Musi obsługiwać protokół BFD</p> <p>Musi przechowywać minimum 128 000 wpisów routingu IPv4 i minimum 64 000 wpisów routingu IPv6</p> <p>Musi wspierać mechanizm ECMP</p> <p>Musi wspierać protokół redundancji VRRP</p> <p>Wsparcie dla DHCP server i DHCP Relay</p> <p>Obsługa Policy Based Routing</p>
Obsługa kolejek	<p>Musi wspierać następujące mechanizmy związane z zapewnieniem, jakości obsługi (QoS) w sieci:</p> <ul style="list-style-type: none"> – Klasyfikacja ruchu dla klas różnej, jakości obsługi QoS poprzez wykorzystanie, co najmniej następujących paramentów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, vlan, wartość DSCP – Implementacja, co najmniej 8 kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. – Implementacja mechanizmu Weighted Random Early Detection (WRED) – Musi wspierać następujące mechanizmy związane z zarządzaniem i zapewnieniem bezpieczeństwa w sieci: – Co najmniej 3 poziomy dostępu administracyjnego przez konsolę: – Autoryzacja użytkowników/portów w oparciu o 802.1x – Obsługa List dostępu ACL dla adresów MAC i adresów IPv4 i IPv6
Zarządzanie i monitoring	<p>Musi wspierać następujące mechanizmy zarządzania:</p> <ul style="list-style-type: none"> – Możliwość uzyskania dostępu do urządzenia przez SNMPv1/2/3 i SSHv2 – Obsługa monitorowania ruchu na porcie (Port Monitoring) – Urządzenie musi posiadać dedykowany port konsolowy do zarządzania typu RJ45 (konsola) oraz drugi wydzielony 10/100/1000BaseT – Plik konfiguracyjny urządzenia musi być możliwy do edycji 'off-line'. Tzn. konieczna jest możliwość przeglądania zmian konfiguracji w pliku tekstowym na dowolnym PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne bez częściowych restartów zarządzania po dokonaniu zmian
Inne	<p>Dodatkowo należy dostarczyć jeden pasywny kabel DAC 100G o długości min. 1m.</p> <p>Urządzenie musi być zamontowane w szafie RACK i uruchomione.</p> <p>Urządzenie musi być skonfigurowane zgodnie ze wskazaniami i uzgodnieniami z Zamawiającym na etapie instalacji. Konfiguracja powinna zapewniać minimum 2 podsieci (VLAN) oraz umożliwiać autoryzację IEEE 802.1x.</p>

2) Przełączniki brzegowe 48 portowy Base-T

Nazwa komponentu	Wymagane minimalne parametry techniczne
------------------	---

Obudowa	Obudowa typu RACK 19"; Wysokość maksymalna 1U; Musi posiadać minimum 2 wymienne moduły zasilacza AC (hot-swap);
Pamięć	Wbudowana pamięć RAM min. 1GB;
Porty	Minimum 48 x 1 Gigabit Ethernet Minimum 4 x 10 Gigabit Ethernet Minimum 1 port konsolowy RJ45 Minimum 1 port -USB
Wydajność	Architektura procesora minimum 4 core i minimum 1GHz Obsługa min. 16 000 adresów MAC; Obsługa min. 4000 sieci VLAN jednocześnie; Rozmiar tablicy ARP minimum: 8 000; Musi obsługiwać, co najmniej protokoły: STP, RSTP, VBST; Musi wspierać funkcjonalność wirtualnej agregacji portów umożliwiającą: - terminowanie pojedynczej wiązki EtherChannel/LACP ;
Routing	Musi obsługiwać protokoły dynamicznego routing dla IPv4 i dla IPv6: OSPF, BGP, IS-IS Musi wspierać mechanizm ECMP Musi wspierać protokół redundancji VRRP Wsparcie dla DHCP server i DHCP Relay Obsługa Policy Based Routing Obsługa min. 8 000 tras dla routingu Ipv4; Obsługa min. 3 000 tras dla routingu Ipv6;
Obsługa kolejek	Musi wspierać następujące mechanizmy związane z zapewnieniem, jakości obsługi (QoS) w sieci: – Klasyfikacja ruchu dla klas różnej, jakości obsługi QoS poprzez wykorzystanie, co najmniej następujących paramentów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP; – Implementacja, co najmniej 8 kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. – Musi wspierać następujące mechanizmy związane z zarządzaniem i zapewnieniem bezpieczeństwa w sieci: – Co najmniej 3 poziomy dostępu administracyjnego przez konsole: – Autoryzacja użytkowników/portów w oparciu o 802.1x – Obsługa List dostępu ACL dla adresów MAC i adresów IPv4 i IPv6
Zarządzanie i monitoring	Musi wspierać następujące mechanizmy zarządzania: – Możliwość uzyskania dostępu do urządzenia przez SNMPv1/2/3 i SSHv2 – Obsługa monitorowania ruchu na porcie (Port Monitoring) – Obsługa funkcjonalności: RMON, sFlow, NTP – Urządzenie musi posiadać dedykowany port konsolowy do zarządzania typu RJ45 (konsola) oraz drugi wydzielony 10/100BaseT – Plik konfiguracyjny urządzenia musi być możliwy do edycji 'off-line'. Tzn.

	konieczna jest możliwość przeglądania zmian konfiguracji w pliku tekstowym na dowolnym PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne bez częściowych restartów urządzenia po dokonaniu zmian
Inne	Urządzenie musi być zamontowane w szafie RACK i uruchomione. Urządzenie musi być skonfigurowane zgodnie ze wskazaniami i uzgodnieniami z Zamawiającym na etapie instalacji. Konfiguracja powinna zapewniać minimum 2 podsieci (VLAN) oraz umożliwiać autoryzację IEEE 802.1x.

3) Urządzenie brzegowe klasy UTM (Unified Threat Management)

Nazwa komponentu	Wymagane minimalne parametry techniczne
Informacje ogólne	<p>Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe.</p> <p>Dopuszcza się, aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia.</p> <p>W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>System musi zapewnić monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.</p> <p>Dostarczone rozwiązanie musi umożliwić łączenie w klastery Active-Active lub Active-Passive każdego z elementów systemu.</p> <p>Systemu ochrony musi realizować funkcjonalności:</p> <ul style="list-style-type: none"> - Kontrola dostępu - zaporę ogniową klasy Stateful Inspection; - Ochrona przed wirusami – antywirus; - Ochrona antyspamowa; - Poufność danych - IPSec VPN oraz SSL VPN; - Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]; - Kontrola stron Internetowych – Web Filter; - Kontrola zawartości poczty – antyspam (dla protokołów SMTP, POP3); - Ochrona przed zagrożeniami typu APT [sandbox]; - Kontrola pasma oraz ruchu [QoS i Traffic shaping]; - Kontrola aplikacji oraz rozpoznawanie ruchu P2P; - Ochronę przed zagrożeniami dnia zerowego (APT); - Analizę ruchu szyfrowanego protokołem SSL. <p>Rozwiązanie musi pozwalać na, wyłączenie / włączenie każdego z modułów rozwiązania, bez restartowania rozwiązania.</p> <p>Wymagane jest automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.</p>
Pamięć	zainstalowane min. dwa dyski 240 GB SSD
Interfejsy	min. 2 porty 10 GE SFP+

	min. 8 portów GE RJ45 min. 8 portów GE SFP min. 2 porty do zarządzania GE RJ45 min. 2 porty USB port do konsoli RJ45
ZASILANIE	Zasilacze redundantne typu Hot Swap o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia, pracujący w sieci 230V 50/60Hz prądu zmiennego wraz z kablem zasilającym o długości minimum 1,5m.
Funkcje bezpieczeństwa	<p>W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:</p> <ul style="list-style-type: none"> - Poufność danych - IPsec VPN oraz SSL VPN - Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3) - Kontrola pasma oraz ruchu [QoS i Traffic shaping] - Kontrola aplikacji oraz rozpoznawanie ruchu P2P - Analiza ruchu szyfrowanego protokołem SSL
Wydajność systemu	przepustowość min. 10 Gbps dla IPS (IPS Throughput) wydajność ochrony przed zagrożeniami min. 7 Gbps (<u>włączony moduł AV</u>) Przepustowość zapory IPv4 min. 36 Gbps Przepustowość IPsec VPN } min. <u>15</u> Gbps Application Control Throughput min. 15 Gbps Sesje równoległe (TCP) min. <u>5</u> Million Nowe sesje/sekundę (TCP) min. <u>150</u> 000
Firewall	Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. Polityki zapory min. <u>5</u> 000 Musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. Urządzenie ma obsługiwać translacje NAT adresu źródłowego i NAT adresu docelowego. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
VPN	Tunele IPsec VPN Gateway-to-Gateway min. 2 000 Tunele IPsec VPN Client-to-Gateway min. 5 000. Użytkownicy równoległe dla SSL-VPN min. 1 000 W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż: <ul style="list-style-type: none"> - Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site; - Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem;

	<ul style="list-style-type: none"> - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności; - Praca w topologii Hub and Spoke oraz Mesh; - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth; - Obsługa ssl vpn w trybach portal oraz tunel
IPS	Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów. Dodatkowo musi być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
ANTYWIRUS	Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 21).
WEB FILTER	Baza filtra WWW pogrupowana w min 50 kategorii tematycznych. W ramach filtra www muszą być dostępne m.in. kategorie spyware, malware, spam, proxy avoidance, sieci społecznościowe, zakupy. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
KONTROLA APLIKACJI	Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
OBSŁUGA ROUTINGU	Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP.
UWIERZYTELNIANIE	<p>System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:</p> <ul style="list-style-type: none"> - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu; - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP; - Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych; <p>Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny;</p>
POLITYKA BEZPIECZEŃSTWA	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).
AKTUALIZACJA	Wymagane jest automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
ZARZĄDZANIE	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.
CERTYFIKATY	Element oferowanego systemu bezpieczeństwa realizujący zadanie Firewall musi posiadać certyfikat ICSA lub EAL4+ dla rozwiązań kategorii Network

	<p>Firewall.</p> <p>W przypadku braku w/w certyfikatów na internetowych stronach producenta, Wykonawca będzie musiał dołożyć dokumenty potwierdzające spełnienie przez produkt wymagań jakościowych.</p>
INSTALACJA I URUCHOMIENIE	<p>Urządzenia musi być dostarczone, zainstalowane w miejscu dostawy, którym jest siedziba Zamawiającego oraz skonfigurowane. Przed rozpoczęciem konfiguracji Zamawiający wymaga przygotowanie przez wykonawcę planu wdrożenia obejmującego projekt struktury WAN oraz procedury bezpieczeństwa. Projekt musi obejmować minimum:</p> <ol style="list-style-type: none"> 1) analizę istniejących rozwiązań brzegowych w Starostwie oraz Jednostkach organizacyjnych; 2) analizę konfiguracji urządzeń uwzględniając adresację urządzeń oraz zastosowane polityki; 3) proponowany schemat połączeń VPN z adresacją urządzeń; 4) schemat VLAN; <p>oraz musi być uzgodniony i zaakceptowany przez Zamawiającego.</p> <p>Konfiguracja musi być przeprowadzona zgodnie z projektem z uwzględnieniem minimalnych prac:</p> <ol style="list-style-type: none"> 1) Weryfikacja założeń wdrożenia 2) Konfiguracja sieci (interfejsy i routing) 3) Konfiguracja firewalla 4) Konfiguracja PAT/NAT/DMZ 5) Konfiguracja IPS – zgodnie z wymaganiami klienta 6) Konfiguracja dodatkowych usług sieciowych tj. DHCP, DNS Proxy 7) Integracja z AD lub założenie wewnętrznej bazy użytkowników (bez dodawania użytkowników). 8) Konfiguracja transparentnej autoryzacji w AD – konfiguracja po stronie urządzenia, inżynier nie instaluje agenta SSO a jedynie instruuje klienta jak powinna przebiegać instalacja. 9) Konfiguracja VPN: <ul style="list-style-type: none"> – IPSec Site-to-Site– zgodnie z otrzymanymi od klienta parametrami tuneli. – IPSec Client-to-Site – konfiguracja urządzenia i wzorcowej stacji klienckiej na kliencie dedykowanym lub ShrewVPN zgodnie z otrzymanymi od Zamawiającego sugestiami dostępu. 10) Konfiguracja SSL VPN lub PPTP VPN. <p>Urządzenie musi zostać podłączone do istniejącej infrastruktury Zamawiającego i uruchomione w celu weryfikacji poprawności konfiguracji.</p> <p>Po zakończonej konfiguracji i przeprowadzeniu testów, wykonawca dostarczy dokumentację zawierającą parametry konfiguracji, hasła oraz raport z testów urządzenia.</p> <p>Wykonawca przeprowadzi instruktarz dla administratora Zamawiającego w zakresie w/w zagadnień, w stopniu umożliwiającym administratorowi samodzielną konfigurację i administrację urządzenia.</p>

4) Oprogramowanie do zarządzania urządzeniami sieci

Nazwa komponentu	Wymagane minimalne parametry techniczne
Informacje ogólne	Oprogramowanie musi umożliwiać zarządzanie wszystkimi urządzeniami sieciowymi dostarczonymi w ramach zamówienia.
Funkcjonalność	<p>Przeglądanie informacji o alarmach kluczowych urządzeń i statusie zasobów.</p> <p>Przegląd kluczowych wskaźników wydajności w całej sieci.</p> <p>Monitorowanie stanu urządzeń w czasie rzeczywistym.</p> <p>Wykrywanie nieprawidłowości i zgłaszanie alarmów.</p> <p>System ma mieć możliwość informowanie o alarmie za pomocą ostrzeżenia dźwiękowego, wiadomości e-mail i SMS.</p> <p>Przeglądanie danych dotyczących wydajności poprzez konsolę zarządzania.</p> <p>Możliwość zapisania wyników jako pliku</p> <p>Monitorowanie wykorzystania procesora i pamięci, łączności urządzenia i czasu reakcji urządzenia w czasie rzeczywistym.</p> <p>Monitorowanie stanu pracy systemów teleinformatycznych i zapobieganie awariom sieci za pomocą wskaźników ruchu, takich jak ruch w porcie i urządzenia TCP, UDP i SNMP.</p> <p>Przeglądanie historycznych danych dotyczących wydajności określonego wskaźnika lub zasobu po zebraniu danych dotyczących wydajności.</p> <p>Ustalanie progów. Jeśli wskaźnik wydajności przekroczy próg, generowany jest alarm, który umożliwia administratorowi monitorowanie nieprawidłowości w czasie rzeczywistym.</p> <p>Wsparcie konfiguracji dostarczonych urządzeń. Konfiguracja parametrów pracy urządzenia, pakietów oprogramowania oraz portów sieciowych.</p> <p>Obsługa konfiguracji urządzeń na podstawie szablonu konfiguracji.</p> <p>Automatyczne łączenie się urządzeń z oprogramowaniem przy użyciu różnych protokołów sieciowych.</p> <p>Wsparcie konfiguracji zasad bezpieczeństwa firewall, zarządzanie wirtualnymi zaporami ogniowymi oraz konfiguracja zasad bezpieczeństwa dla wirtualnych zapor ogniowych.</p> <p>Obsługa aktualizacji oprogramowania urządzeń sieciowych.</p> <p>Tworzenie kopii zapasowych, przywracanie, porównywanie konfiguracji, umożliwiające użytkownikom szybkie lokalizowanie usterek i przywracanie do określonej fazy.</p> <p>Możliwość tworzenia raportów.</p> <p>Dynamicznie wyświetlane danych i analiz, pomagające użytkownikom przewidzieć trendy danych usług.</p> <p>Udostępniać i obsługiwać urządzenia i usługi sieciowe: zasady bezpieczeństwa i QoS, dostęp przez sieć VPN oraz raportowanie;</p> <p>Monitorować i wyświetlać statystyki ruchu sieciowego zgodnie z parametrami ustawianymi przez użytkownika itp.</p> <p>Udostępniać i zarządzać bezprzewodowymi kontrolerami dostępu, punktami dostępu i urządzeniami sieci LAN; zapewnia rozwiązywanie problemów i konserwację.</p>

	5 lat suportu i dostępu do aktualizacji.
--	--