OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa sprzętu komputerowego i oprogramowania.

Dostawa dotyczy: sprzętu komputerowego, sprzętu sieciowego, akcesoriów komputerowych, kserografów, serwera blade, oprogramowania oraz licencji..

Szczegółowy opis przedmiotu zamówienia:

I	**Stacja robocza o parametrach nie gorszych niż:**	3 szt.
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzeń
1.	Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta
2.	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych
3.	Procesor	Procesor taktowany zegarem co najmniej 3,2 GHz, pamięci cache L3 6MB oraz powinien osiągać w teście wydajności PassMark PerformanceTest (wynik dostępny: http://www.passmark.com/products/pt.htm) co najmniej wynik 6600 punktów Passmark CPU Mark
4.	Pamięć operacyjna RAM	Pamięć operacyjna: min. 4GB 1600 MHz możliwość rozbudowy do min 32GB
5.	Parametry pamięci masowej	Min. 500 GB SATA, 7200 obr./min . zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników..
6.	Grafika	Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową ze wsparciem dla DirectX 10.1, OpenGL 3.0, Shader 4.1 – z możliwością dynamicznego przydzielenia do 1,5GB pamięci.
7.	Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, porty słuchawek i mikrofonu na przednim oraz na tylnym panelu obudowy.
8.	Obudowa	Typu SFF z obsługą kart PCI 32bit oraz PCI Express wyłącznie o niskim profilu, wyposażona w min. 3 kieszenie: 1 szt 5,25” zewnętrzna, 1 szt 3,5” wewnętrzna i 1 szt 3,5” zewnętrzna. Zasilacz o mocy minimum 280W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 86%, przy 50% obciążeniu. W celu szybkiej weryfikacji usterki w obudowę komputera musi być wbudowany akustyczny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami;
9.	Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 7 32bit i 64bit (dopuszcza się wydruk ze strony Microsoft WHCL)
10.	Bezpieczeństwo	Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego.

11.	BIOS	Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: • wersji BIOS, • ilości i sposobu obłożenia slotów pamięciami RAM, • typie procesora wraz z informacją o ilości rdzeni, wielkości pamięci cache L1, L2 i L3, pojemności zainstalowanego dysku twardego • rodzajach napędów optycznych • MAC adresie zintegrowanej karty sieciowej • kontrolerze audio Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS) Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość ustawienia następujących zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora. Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowy tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, modułu TPM, portu równoległego, portu szeregowego z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. Możliwość wyłączania portów USB w tym: wszystkich portów, tylko portów znajdujących się na przedzie obudowy, tylko tylnych portów.
12.	Dodatkowe oprogramowanie	Oprogramowanie dostarczone przez producenta komputera pozwalające na zdalną inwentaryzację komputerów w sieci, lokalną i zdalną inwentaryzację komponentów komputera, umożliwiające co najmniej: Zdalne wyłączanie i restart komputera w sieci, Monitorowanie stanu komponentów: CPU, Pamięć RAM, HDD, wersje BIOS, Tworzenie indywidualnych numerów dla poszczególnych użytkowników, Włączenie lub wyłączanie BOOTowania portów USB Zdalne zarządzanie energią urządzeń. W pełni automatyczną instalację sterowników urządzeń opartą o automatyczną detekcję posiadanego sprzętu
13.	Certyfikaty i standardy	Komputery mają spełniać normy i posiadać deklaracje zgodności (lub inne dokumenty potwierdzające spełnienie norm) w zakresie: • Deklaracja zgodności CE • normy Energy Star 5.0 • Certyfikat EPEAT na poziomie GOLD • Wymagany wpis dotyczący oferowanego modelu komputera w internetowym katalogu http://www.eu-energystar.org lub http://www.energystar.gov – dopuszcza się wydruk ze strony internetowej • Wymagany wpis dotyczący oferowanego modelu komputera w internetowym katalogu http://www.epeat.net - dopuszcza się wydruk ze strony internetowej • Być wykonane/wyprodukowane w systemie zapewnienia jakości ISO 9001 Dla potwierdzenia, że oferowany sprzęt odpowiada postawionym wymaganiom i był

		wykonany przez Wykonawcę (a jeżeli Wykonawca nie jest producentem to przez producenta) w systemie zapewnienia jakości wg normy ISO 9001 aby Wykonawca posiadał :Certyfikat ISO 9001 lub inne zaświadczenie/dokument wydane przez niezależny podmiot zajmujący się poświadczaniem zgodności działań wykonawcy z normami jakościowymi -odpowiadającej normie ISO 9001- (wymagany dokument potwierdzający spełnianie wymogu). Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia wykonawcy (wymagane potwierdzenie spełnienia wymogu).
14.	Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie jałowym (IDLE) wynosząca maksymalnie 23 dB Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń i napędów bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych); Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych). Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki).
15.	Warunki gwarancji	Na okres co najmniej 36 miesięcy - świadczonej w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta ,lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca Czas reakcji na zgłoszoną reklamację gwarancyjną - do końca następnego dnia roboczego W przypadku naprawy trwającej dłużej niż 48 godzin, zamawiającemu musi zostać dostarczony komputer zastępczy Naprawy gwarancyjne urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta, W przypadku awarii dysku twardego, dysk pozostaje u Zamawiającego Wykonawca wraz ze sprzętem dostarczy dokument potwierdzający udzielenie gwarancji przez producenta sprzętu (karta gwarancyjna producenta).
16.	Wsparcie techniczne producenta	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera –
17.	Wymagania dodatkowe	Zainstalowany system operacyjny Microsoft Windows 7 Professional (64-bit), nie wymagający aktywacji za pomocą telefonu lub Internetu w firmie Microsoft wraz z nośnikiem. Wbudowane porty: - Wbudowane porty minimalnie: - 1 x VGA - 1 x DVI - 1 x RS-232 - 1 x LPT - 1 x eSATA - 2 x PS/2 - 1 x RJ-45 - 1 x Audio: line-in - 1 x Audio: line-in/mikrofon - 1 x Audio: line-out - 1 x Audio: mikrofon z przodu obudowy - 1 x Audio: słuchawki z przodu obudowy - 12 szt USB w tym: minimum 2 porty z przodu obudowy, minimum 6 portów z tyłu obudowy (w tym min. 2 x USB 3.0), minimum 4 porty wewnątrz

		obudowy. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
		- Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika)
		- Płyta główna z wbudowanymi:
		  - 1 złącze PCI (32-bit/33 MHz)
		  - 2 złącza PCI-Express x1
		  - 1 złącze PCI-Express 3.0 x16
		Obsługa kart wyłącznie o niskim profilu – nie dopuszcza się kart o profilu pełnym, minimum 4 złącza DIMM z obsługą do 32GB DDR3 pamięci RAM, min. 4 złącz SATA NCQ w tym min 1 złącze SATA 3.0,
		Klawiatura USB w układzie polski programisty
		Mysz optyczna USB z dwoma klawiszami oraz rolką (scroll)
		Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania i odtwarzania płyt
		Dołączony nośnik ze sterownikami

II	**Monitor 23” o parametrach nie gorszych niż:**	3 szt.
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzeń
1.	Typ ekranu	Panoramiczny; ciekłokrystaliczny z aktywną matrycą TN
2.	Rozmiar plamki	Maks. 0.277 mm
3.	Jasność	min. 250 cd/m2
4.	Kontrast	Min. 1000:1
5.	Kąty widzenia (pion/poziom)	Min. 176°/170 stopni
6.	Czas reakcji matrycy	Maks. 5ms
7.	Zalecana rozdzielczość obrazu	1600 x 900
8.	Powłoka powierzchni ekranu	Przeciwodblaskowa
9.	Częstotliwość odświeżania poziomego	20-90 kHz
10.	Częstotliwość odświeżania pionowego	60-70 Hz
11.	Podświetlenie	System podświetlenia LED
12.	Zakres pochylenia monitora	Od -5° do +15°
13.	Bezpieczeństwo	Monitor musi być wyposażony w tzw. Kensington Slot
14.	Waga bez podstawy	Maksymalnie 3,5 kg
15.	Złącza	2 x HDMI, 15-stykowe D-Sub, Wyjście SPDIF, 1 x wejście audio (stereo mini-jack)

16.	Dodatkowe	Monitor musi posiadać usuwalną podstawę montażową, wbudowane 2 głośniki min. 1,5W; kompatybilność z VESA 100mm
17.	Gwarancja	Na okres co najmniej 36 miesięcy - świadczonej w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca Czas reakcji na zgłoszoną reklamację gwarancyjną - do końca następnego dnia roboczego W przypadku naprawy trwającej dłużej niż 48 godzin, zamawiającemu musi zostać dostarczony monitor zastępczy Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta, Wykonawca wraz ze sprzętem dostarczy dokument potwierdzający udzielenie gwarancji przez producenta sprzętu (karta gwarancyjna producenta).
18.	Certyfikaty	Monitory muszą być wykonane zgodnie normami i posiadać Certyfikaty: TCO 5.1, ISO9241-307, EPEAT Silver, Energy Star 5.0 – lub inne dokumenty wdane przez niezależny podmiot uprawniony do kontroli jakości, potwierdzające, że dostarczone monitory odpowiadają wskazanym normom.
19.	Zużycie energii	Średnie użycie energii 21W, Max 24W Mniej niż 1W – tryb uśpienia

III	**Zasilacz awaryjny UPS o parametrach nie gorszych niż:**	4 szt.
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzeń
1.	Moc wyjściowa	Min. 300 W / 500 VA.
2.	Maksymalna moc, jaką można skonfigurować	Min. 300 W / 500 VA.
3.	Napięcie wyjściowe	230 V.
4.	Gniazda wyjściowe	Min. 1 IEC 320 C13 (Ochrona przeciwprzepięciowa). 
		Min. 3 IEC 320 C13 (Zasilanie zapasowe). 
5.	Nominalne napięcie wejściowe	230 V.
6.	Częstotliwość na wejściu	50/60 Hz +/- 3 Hz.
7.	Typ gniazda wejściowego	IEC-320 C14.
8.	Zakres napięcia wejściowego w trybie podstawowym	180 – 280 V.
9.	Zmienny zakres napięcia wejściowego w trybie podstawowym	160 – 280 V.
10.	Typ akumulatora	Bezobsługowe baterie ołowiowo-kwasowe.

11.	Typowy czas pełnego ładowania akumulatora	Do 6 godzin.
12.	Typowy czas podtrzymania przy obciążeniu 200W	Min. 8 minut.
13.	Typowy czas podtrzymania przy pełnym obciążeniu 300 W	Min. 4 minuty..
14.	Port komunikacyjny	USB.
15.	Panel przedni	Diody LED wskazują pracę z sieci : pracę z baterii : stan wymiany baterii : wskaźniki stanu przeciążenia.
16.	Funkcje monitorowania	Temperatura pracy urządzenia, przewidywany czas podtrzymania, kalibracja realnego czasu podtrzymania napięcia poprzez oprogramowanie producenta.
17.	Alarm dźwiękowy	Alarm podczas pracy na baterii: znaczny stan wyczerpania baterii : ciągły sygnał dźwiękowy w stanie przeciążenia.
18.	Znamionowa energia przepięcia (w dżulach)	Do 300 Dżule (J).
19.	Potwierdzenia zgodności	C-tick, CE, GOST, VDE.
20.	Okres gwarancji	Min. 24 miesiące naprawy albo wymiany. Wykonawca wraz ze sprzętem dostarczy dokument potwierdzający udzielenie gwarancji przez producenta sprzętu (karta gwarancyjna producenta).

IV	**Kolorowa drukarka laserowa o parametrach nie gorszych niż:**	5 szt.
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzeń
1.	Technologia Druku	Laserowa, kolorowa.
2.	Rozdzielczość	600x600 dpi.
3.	Prędkość druku	czarny: min 14 str.A4/ kolor: min. 14 str. A4/min.
4.	Procesor	Min. 700MHz.
5.	Pamięć	Min. 128 MB
6.	Porty	USB 2.0, Ethernet
7.	Karta sieciowa	Wewnętrzna, 10/100 Base-TX.
8.	Języki drukowania	PCL5c, PCL6, Postscript 3 lub emulacje.
9.	Druk dwustronny	Ręczny (obsługa druku dwustronnego w sterowniku drukarki).
10.	Wymiary nośników	A4, A5, A6, B5 (JIS); 10 x 15 cm, kartki pocztowe (pojedynczy i podwójny format JIS); koperty (DL, C5, B5). Od 76 x 127 do 216 x 356 mm
11.	Podajniki papieru	Min. 1, pojemność min. 150 arkuszy
12.	Odbiornik papieru	Min. 125 arkuszy.
13.	Gramatura nośników	Min. 200 g/m2.
14.	Nośniki	Papier (typu bond, broszurowy, kolorowy, błyszczący, ciężki, firmowy, lekki, fotograficzny, zwykły, wstępnie zadrukowany, dziurkowany, makulaturowy, szorstki), folie, etykiety, koperty, kartki.

15.	Sterowniki	Microsoft® Windows® 7 w wersji 32- i 64-bitowej, Windows Vista® w wersji 32- i 64-bitowej, Windows® XP w wersji 32-bitowej (z dodatkiem SP2 lub nowszym); Instalacja samych sterowników obsługiwana w systemach: Microsoft® Windows® Server 2008 w wersji 32- i 64-bitowej, Windows® Server 2003 w wersji 32-bitowej (z dodatkiem SP3 lub nowszym)
16.	Wymiary (sz. x gł. x wys.)	Maks. 420 x 470 x 260 mm.
17.	Waga	Poniżej 20 kg
18.	Pobór mocy	Poniżej 330 W
19.	Gwarancja producenta na urządzenie	Min. 24 miesięczna gwarancja w miejscu instalacji. Wykonawca wraz ze sprzętem dostarczy dokument potwierdzający udzielenie gwarancji przez producenta sprzętu (karta gwarancyjna producenta).
20.	Materiały eksploatacyjne	Dostarczone materiały eksploatacyjne (toner, bęben) muszą być nowe, tego samego producenta, co urządzenie.

V	**Urządzenie wielofunkcyjne o parametrach nie gorszych niż:**	5 szt.
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzeń
1.	Technologia Druku	Laserowa, kolorowa.
2.	Funkcje standardowe	Drukowanie, kopiowanie, skanowanie, faksowanie.
3.	Prędkość drukowania (A4)	Kolor: min. 35 str./min, Czarny: min. 35 str./min.
4.	Prędkość kopiowania	min. 35 str./min - Simplex min. 24 str./min - Duplex
5.	Druk dwustronny	Automatyczny (Standard).
6.	Maksymalne dopuszczalne obciążenie	Min. 75 000 stron miesięcznie.
7.	Czas wydrukowania pierwszej strony, drukowanie	Maks. 9 sekund czarno-białe / maks. 10 sekund kolor.
8.	Czas wydrukowania pierwszej strony, kopiowanie	Maks. 13 sekund czarno-białe / maks. 16 sekund kolor.
9.	Rozdzielczość wydruku	Min. 600 x 600 dpi.
10.	Pamięć drukowania	Min. 512 MB. z możliwością rozbudowy do 1GB
11.	Procesor	Min. 500 MHz.
12.	Podłączenie	Prędkość 10/100/1000 Ethernet, USB 2.0
13.	Docelowe miejsca skanowania	Skanowanie do pamięci USB, Skanowanie do komputera z wykorzystaniem SMB, Skanowanie na adres email z wykorzystaniem LDAP, Skanowanie do serwera z wykorzystaniem FTP
14.	Języki opisu strony (PDL)	PCL® 5, PCL® 6, PDF emulacja, True Adobe® PostScript® 3™, XPS lub równoważne.
15.	Funkcje kopiowania	Kopiowanie jednostronnych oryginałów na dwustronne kopie, Auto dopasowanie, klonowanie, Układanie, Usuwanie brzegu, Kopiowanie dowodów osobistych, N-stron, Zmniejszanie/Powiększanie

16.	Opcje faksu	Książka adresowa, Emisja faksów, Wysyłanie z opóźnieniem, Unikalny dzwonek, Przekazywanie faksu na e-mail, Przesyłanie faksu do innych terminali, w formie wiadomości, na serwer (FTP, SMB), Blokada spamu, Polling,.
17.	Formaty plików skanowania	Co najmniej: JPEG, PDF, TIFF.
18.	Kolorowe skanowanie	Tak.
19.	Funkcje e-mail	Bezpośrednie wysyłanie wiadomości e-mail z urządzenia.
20.	Pojemność na papier	podajnik na min. 550 arkuszy, podajnik boczny na min. 150 arkuszy.
21.	Automatyczny podajnik dokumentów	Automatyczny podajnik dokumentów do druku dwustronnego Wydajność: 50 arkuszy.
22.	Obsługiwany rozmiar papieru	Taca (Taca wielozadaniowa): Rozmiary niestandardowe: od min. 76.2 x 127 mm do 216 x 356 mm Taca 1: Rozmiary niestandardowe: od min. 148 x 210 mm do 216 x 356 mm.
23.	Obsługiwana gramatura papieru	Zakres min. 60-210 g/m².
24.	Obsługiwane typy nośników	Taca (Taca wielozadaniowa): Papier na wizytówki, Karton, Koperty, Błyszczący, Etykiety, Zwykły papier Taca 1: Papier na wizytówki, karton, błyszczący, zwykły papier.
25.	Pojemność tacy wyjściowej	Min. 250 arkuszy.
26.	Obsługiwane systemy operacyjne	Windows® 2003 Server, Windows® 2008 Server, Windows® 7, Windows® Vista, Windows® XP lub nowsze.
27.	Wymagania elektryczne	sieciowe AC (220-240V), 50/60 Hz
28.	Maksymalne zużycie energii (tryb pracy)	580 W.
29.	Maksymalne zużycie energii (tryb oczekiwanie)	80 W.
30.	Maksymalne zużycie energii (tryb energooszczędny)	10 W.
31.	Gwarancja	Min. 36 miesięcy w miejscu instalacji. Zamawiający wymaga, aby sprzęt dostarczony w ramach realizacji umowy posiadał świadczenia gwarancyjne oparte na oficjalnej gwarancji świadczonej przez producenta sprzętu. Wykonawca wraz ze sprzętem dostarczy dokument potwierdzający udzielenie gwarancji przez producenta sprzętu (karta gwarancyjna producenta).

VI	**Ksero A3 o parametrach nie gorszych niż:**	3 szt.
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzeń
1.	Technologia druku	laserowa bez developera jako materiału eksploatacyjnego
2.	Funkcje standardowe	kopiowanie i drukowanie monochromatyczne, skanowanie sieciowe kolorowe
3.	Prędkość drukowania	Min. 25 str. A4/min. – A4 Min. 14 str. A4/min. – A3

4.	Prędkość kopiowania	Min. 25 str. A4/min. – A4 Min. 14 str. A4/min. – A3
5.	Druk dwustronny	automatyczny (duplex) w standardzie
6.	Maksymalne dopuszczalne obciążenie	Do 100 000 stron miesięcznie
7.	Czas wydrukowania pierwszej strony, drukowanie	Min 12s
8.	Czas wydrukowania pierwszej strony, kopiowanie	Min 5s
9.	Rozdzielczość wydruku	Co najmniej 1200x1200 dpi
10.	Rozdzielczość skanowania w trybie mono/kolor	Co najmniej 600x600 dpi
11.	Pamięć drukowania	Min. 1 GB. Wbudowany dysk twardy z co najmniej 160 GB z automatycznym szyfrowaniem.
12.	Procesor	Min. 667 MHz
13.	Podłączenie	USB 2.0, Ethernet 10/100/1000Base-TX Ethernet
14.	Docelowe miejsca skanowania	Skanowanie sieciowe, skanowanie na dysk, skanowanie do poczty e-mail
15.	Języki opisu strony (PDL)	PCL® 5e, PCL 6, HP-GL / HP-GL2, TIFF/PDF, XPS® lub równoważne
16.	Funkcje kopiowania	Adnotacja, Automatyczne zmniejszanie/powiększanie, Automatyczne wybieranie tac, Automatyczne drukowanie 2-stronne, Eliminacja tła, Kopiowanie książek, Tworzenie broszury, Tworzenie pracy, Okładki, Usuwanie w ramach/poza edycją, Elektroniczne układanie wstępne, Form overlay, Kopiowanie dowodów osobistych, Wkładki, Obraz lustrzany, Oryginały o różnych rozmiarach, N-stron, Obraz negatywowy, Page layout, Tryb plakatu, Zestaw próbkowy, Znaki wodne
17.	Formaty plików skanowania	PDF, PDF (przeszukiwalny), PDF (A-1 Level A), TIFF v.6, JFIF, JPEG, XPS
18.	Funkcje e-mail	Bezpośrednie wysyłanie wiadomości e-mail z urządzenia.
19.	Pojemność na papier	Taca boczna min. 50 arkuszy Tace dolne uniwersalne (A4/A3) nr 1 i 2 min. po 500 arkuszy każda
20.	Automatyczny podajnik dokumentów	Podajnik dokumentów do skanowania - dwustronny automatyczny na min. 110 arkuszy.
21.	obsługiwany rozmiar papieru:	automatyczny podajnik: od 85 x 125 mm do 297 x 432 mm (simplex); od 110 x 125 mm do 297 x 432 mm (duplex) Taca boczna: Od 89 x 98 mm do 297 x 432 mm Tace dolne 1 i 2: Od 140 x 182 mm do 297 x 432 mm
22.	Maksymalna gramatura papieru:	automatyczny podajnik: Od 38 do 128 g/m2 (simplex); Od 50 do 128 g/m2 (duplex) Taca boczna: Od 60 do 215 g/m2 Tace dolne: Taca 1: 60 to 105 g/m2 Taca 2: 60 to 215 g/m2

23.	Obsługiwane typy nośników	Taca boczna: Kserograficzny, Papier na wizytówki, Karton, Koperty, Błyszczący, Etykiety, Zwykły papier Tace dolne 1 i 2: Kserograficzny, Papier na wizytówki, Karton, Błyszczący, Zwykły papier.
24.	Pojemność tacy wyjściowej	Podwójna taca wyjściowa po 250 arkuszy każda
25.	Obsługiwane systemy operacyjne	Microsoft® Windows® XP SP3 (32- and 64-bit), Windows Server 2003 (32- and 64-bit), Windows Vista(32- and 64-bit), Windows Server 2008 (32- and 64-bit), Windows 7 (32- and 64-bit)
26.	Wymagania elektryczne	Wejście: 220–240 V, 50/60 Hz Osiągnięcie stanu pracy po włączeniu maks. 40s Przejście w stan pracy ze stanu energooszczędnego maks 12s
27.	Maksymalne zużycie energii (tryb pracy)	Maks. 730W
28.	Maksymalne zużycie energii (tryb oczekiwanie)	Maks. 125W
29.	Maksymalne zużycie energii (tryb energooszczędny)	Maks. 90W
30.	Dodatkowe	Podstawa pod urządzenie Kolorowy panel dotykowy LCD w języku polskim Możliwość logowania indywidualnego (kody dostępu)
31.	Gwarancja	Gwarancja musi obejmować czas minimum 36 miesiące od daty uruchomienia urządzeń w siedzibie Zamawiającego. Wymagany przez Zamawiającego czas reakcji na serwis dla oferowanych urządzeń najpóźniej do końca następnego dnia roboczego, licząc od chwili zgłoszenia telefonicznego. Naprawy gwarancyjne, wizyty diagnostyczne serwisantów oraz usługi świadczone przez Wykonawcę w ramach serwisu gwarancyjnego nie mogą być obciążone kosztami dojazdu do siedziby Zamawiającego. Wykonawca wraz ze sprzętem dostarczy dokument potwierdzający udzielenie gwarancji przez producenta sprzętu (karta gwarancyjna producenta).

VII	**Obudowa typu blade o parametrach nie gorszych niż:**	1 szt.
Lp	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzenia
1.	Typ obudowy	• do montażu w szafie 19” rack; • maksymalna masa obudowy przy dowolnej konfiguracji nie może przekraczać 200kg; • wysokość nie więcej niż 10U dla kompletnej obudowy wraz z wymaganymi modułami chłodzenia, zasilania itp.
2.	Architektura serwerów, możliwości rozbudowy	• możliwość instalacji co najmniej 16 niezależnych serwerów kasetowych wyposażonych w 2 procesory 6 rdzeniowe oraz nie mniej niż 192GB pamięci operacyjnej RAM DDR3 na każdy serwer; • możliwość instalacji kaset typu storage wyposażonych minimum w 4 dyski SAS 2.0 każdy, współdzielenie zasobów każdej kasety dyskowej co najmniej dla 2 serwerów w obrębie tej samej obudowy blade; • możliwość instalacji kaset typu storage wyposażonych w napęd w standardzie LTO-4 lub nowszym.
3.	Architektura I/O	• pełne wsparcie producenta obudowy dla instalacji switchy i kart 10Gbit

		LAN oraz Infiniband; • w ramach jednej obudowy wymagane minimum 8 wnęk do instalacji modułów komunikacyjnych typu przełącznik LAN 1Gbit/s, 10Gbit/s, FC 8Gbit, FC pass-thru, QDR InfiniBand 40Gbit.
4.	Sposób wyprowadzeń sygnałów LAN, FC, IB	• Zainstalowane redundantne moduły pass-thrugh 10Gbit zapewniające możliwości wyprowadzenia co najmniej 2 fizycznych kanałów 10Gbps Ethernet dla każdego serwera blade. Moduły sumarycznie powinny umożliwiać podłączenie do zewnętrznego środowiska sieciowego poprzez min. 32 portów w standardzie 10Gb MMF LC SFP+ • redundantne switche FC wyposażone w minimum 8 wkładek SFP+. Zainstalowane minimum dwa switche FC 8Gb umożliwiające wyprowadzenie po przez backplain co najmniej 36 kanałów FC 8Gb (po 2 na każdy serwer). Każdy ze switchy powinien umożliwiać podłączenie do zewnętrznego środowiska sieciowego poprzez minimum 8 kanałów FC 8Gb, dostarczona licencja na minimum 14 aktywnych portów w każdym switchu. Możliwość rozbudowy poprzez zakup licencji do pełnych 24 portow/switch. Każdy switch dostarczony z minimum 4 - adapterami typuSFP+, 8 Gbit/sec SWL, LC connector, licencja dla Full Fabric.
5.	Zarządzanie	Wymaga się, aby dostarczone rozwiązanie było wyposażone w kartę zarządzającą (tzw. Management blade wyposażoną w: • pełna administracja chassis za pośrednictwem interfejsu Web; • dedykowany port serwisowy LAN RJ-45 dla każdej karty zarządzającej; • funkcję KVM realizowaną dla każdego z serwerów; • minimum dwa porty zarządzające zgodne z warstwą 2+ o prędkości 1Gbit/s; • wsparcie dla LDAP i ADS; • możliwość łączenia minimum 4 obudów blade oraz zarządzania całością z pozycji dowolnie wybranego Management Blade. Wymagane funkcjonalności: • możliwość, weryfikacji zużycia energii całego chassis, konfiguracji polis ograniczających zużycie energii w czasie oraz na bazie raportów wizualnych utylizacji i zużycia energii przez pojedyncze serwery blade jak i całą obudowę w czasie; • obudowa blade musi być dostarczona w konfiguracji umożliwiającej, bez konieczności rozbudowy o dodatkowe elementy sprzętowe, wirtualizację zasobów I/O dla całej obudowy blade (co najmniej wirtualizacja adresacji WWN dla FC; MAC i IP dla Ethernet dla serwerów zainstalowanych w obudowie); • dostarczona infrastruktura serwerowa powinna pracować bez przerw czy obniżenia wydajności serwerów nawet w przypadku uszkodzenia obydwóch modułów zarządzających; • dostarczone rozwiązanie musi umożliwiać zdalne mapowanie napędów optycznych CD/DVD oraz FDD lub obrazów (ISO/IMG) tychże nośników niezależnie dla każdego z zainstalowanych w obudowie serwerów kasetowych na poziomie sprzętowym; • dostarczone rozwiązanie musi umożliwiać zdalne przekierowanie konsoli graficznej każdego z zainstalowanych w obudowie serwerów na poziomie sprzętowym wraz z emulacją myszy i klawiatury (niezależnie od typu zainstalowanego OS), połączenie szyfrowane SSL/SSH; • Zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego; • Chassis wyposażone w wyświetlacz dostępny z przodu obudowy, zapewniający podstawową konfigurację chassis, monitorowanie podstawowych funkcji oraz sygnalizowanie i wyświetlanie alarmów; wyświetlacz musi posiadać możliwość schowania/zamknięcia lub innego skutecznego zabezpieczenia przed przypadkowym uszkodzeniem;

		• Zdalne włączanie/wyłączanie/restart niezależnie dla każdego serwera; • Dostęp do interfejsu zarządzania - zdalny z poziomu przeglądarki internetowej, bez konieczności instalacji specyficznych komponentów programowych producenta sprzętu; • Automatyczne wykrywanie i identyfikacja urządzeń zainstalowanych w ramach infrastruktury (serwery, obudowy blade, karty zarządzające) i prezentacja infrastruktury w postaci graficznej; • Monitorowanie utylizacji następujących podzespołów serwera: procesor, pamięć, dyski twarde, interfejsy sieciowe.
6.	Zasilanie	• Zasilacze wymienne w trakcie pracy, pozwalające na zasilenie w pełni obsadzonej obudowy blade; • Obudowa powinna umożliwiać optymalizowanie obciążenia zainstalowanych zasilaczy celem osiągnięcia maksymalnej sprawności pracy zasilaczy i minimalizacji zużycia energii; • Sprawność maksymalna pojedynczego zasilacza nie mniej niż 90%; • Zasilacz powinien posiadać wizualna sygnalizację stanu pracy – (poprawna praca/ usterka); • Stan i parametry pracy muszą być monitorowane zdalnie (przez kartę zarządzającą) i lokalnie (panel LCD); • Każdy z zasilaczy musi realizować funkcję auto-restart.
7.	Chłodzenie	• Obudowa wyposażona w redundantne chłodzenie (wentylatory) umożliwiające poprawną pracę w pełni wyposażonej obudowy blade; • Obudowa musi umożliwiać wymianę modułów wentylatorów w trakcie pracy; • Każdy moduł chłodzenia wymienny hot-plug powinien posiadać wizualną sygnalizację stanu pracy – (poprawna praca / usterka).
8.	Gwarancja	5 lat gwarancji producenta, w miejscu instalacji u Zamawiającego, z czasem reakcji w następnym dniu roboczym. Dostępność części zamiennych przez 5 lat od momentu zakończenia produkcji (wymagane oświadczenie producenta dostarczone wraz ze sprzętem). Wykonawca wraz ze sprzętem dostarczy dokument potwierdzający udzielenie gwarancji przez producenta sprzętu (karta gwarancyjna producenta).
9.	Inne	• Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane (wymagane oświadczenie producenta dostarczone wraz ze sprzętem) oraz muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne; • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce - Wymagane dostarczenie wraz ze sprzętem oświadczenia producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg.

VIII	**Serwer typu blade o parametrach nie gorszych niż:**	3 szt.
Lp	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzeń
1.	Obudowa	• typu blade, zgodna z zaoferowaną obudową blade, dostarczona przez jednego producenta, serwery zainstalowane w obudowie; • możliwość instalacji 2 dysków SATA/SAS 2.0/ SSD, hotplug w obudowie serwera; • dioda pozwalająca na wizualną identyfikację serwera w obudowie; • diodowa sygnalizacja: pracy, usterki, aktywności połączeń LAN;
2.	Procesory	• Zainstalowane dwa procesory 8-rdzeniowe taktowane zegarem min.

		2,10GHz, 20MB Cache, osiągające co najmniej 556 punktów w teście SPECint_rate2006; • Wymagane dostarczenie pełnego protokołu z testów SPEC poświadczonego przez producenta serwera lub wymagana obecność certyfikatu potwierdzającego osiągnięty wynik na stronie: www.spec.org
3.	Płyta główna	• Obsługa minimum dwóch procesorów ośmiordzeniowych; • Obsługa minimum 384 GB pamięci operacyjnej typu DDR3 z technologiami Advanced ECC, Chipkill (SDDC), wsparcie dla trybu aktywnej rezerwy i zapisu lustrzanego pamięci RAM; • Wyposażona w zintegrowany kontroler SAS 2.0 RAID 0/1; • Zaprojektowana i wyprodukowana przez producenta serwera; • Dwa złącza dla kart nakładkowych FC/Ethernet 10Gbit/IB typu mezzanine PCI Express gen. 3.0 x8 i dodatkowe złącze PCI Express gen.3 x8 na kontroler RAID; • wsparcie dla TPM 1.2 (możliwość integracji); • możliwość instalacji modułu flash do obsługi wirtualizatora (wewnętrzne złącze typu USB, niedostępne z zewnątrz serwera);
4.	Pamięć RAM	Wyposażony w minimum 32GB DDR3
5.	Zintegrowane dyski / pamięć	Zintegrowana pamięć wewnętrzna serwera typu flash min. 2GB
6.	Interfejsy I/O , złącza	• Minimum 2 interfejsy LAN typu 10 Gbit/s ze wsparciem technologii Intel VT-c lub równoważnej podłączone poprzez backplane do switchy zainstalowanych w obudowie blade; • Dedykowany interfejs serwisowy typu LAN 100Mbit/s do obsługi i konfiguracji sprzętowej karty zarządzającej, możliwość przejęcia funkcji dedykowanego interfejsu serwisowego przez jeden z podstawowych interfejsów LAN 10 Gbit/s; • min 2 interfejsy FC 8Gbit podłączone poprzez backplane do switchy zainstalowanych w obudowie blade;
7.	Oprogramowanie	Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, 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 (temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).
8.	Zarządzanie	• Zintegrowany z płytą główną kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający zdalny restart serwera i pełne zarządzanie włącznie z przejęciem zdalnym konsoli graficznej oraz zdalnego podłączenia napędów na poziomie sprzętowym; • Dedykowana karta LAN 10/100 Mb/s do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym serwera; • Umieszczona z przodu chowana karta identyfikacyjna serwera zawierająca nazwę serwera, numer seryjny, adresy MAC wbudowanych kart sieciowych;
9.	Gwarancja	5 lat gwarancji producenta, w miejscu instalacji u Zamawiającego, z czasem reakcji w następnym dniu roboczym. Dostępność części zamiennych przez 5 lat od momentu zakończenia produkcji (wymagane oświadczenie producenta dostarczone wraz ze sprzętem). Wykonawca wraz ze sprzętem dostarczy dokument potwierdzający udzielenie gwarancji przez producenta sprzętu (karta gwarancyjna producenta).
10.	Inne	• Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane (wymagane oświadczenie producenta) oraz muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne; • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału

		dystrybucyjnego w Polsce - Wymagane dostarczenie wraz ze sprzętem oświadczenia producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg; • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera.

IX	**System bezprzewodowego i przewodowego zarządzania siecią**	
Nazwa komponentu		Ilość
Serwerowy przełącznik agregacyjny(TOR)		1 szt.
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzenia
1.	Porty	• Min. 24 porty 1000/10 GBaseX (SFP+) • Min. 4 porty uplink 40Gb QSFP+
2.	Zamocowanie	Standardowy stelaż 19”
3.	Pamięć i procesor	Minimalna wielkość bufora pakietów 9 MB
4.	Przepustowość	Minimalna przepustowość 595 Mpps
5.	Wydajność	Minimalna wydajność 800 Gbps
6.	Funkcje zarządzania	Przełącznik musi obsługiwać następujące funkcjonalności: • SNMP v1/v2c/v3 • Interfejs zarządzania sieci Web • Standardowy interfejs wiersza poleceń CLI • Zarządzanie IPv4/IPv6 • Zarządzanie wieloma kontami użytkowników lokalnych • Obsługa wielu obrazów oprogramowania z funkcją odtwarzania • Obsługa wielu plików konfiguracyjnych • Plik konfiguracyjny w formie edytowalnej (Boot Prom) oraz pobieranie oprogramowania firmware przez port szeregowy • Telnet Server/Client • Secure Shell (SSHv2) Server/Client • Syslog • Audit Trail Logging • Obsługa FTP/TFTP Client • Simple Network Time Protocol (SNTP) lub NTP • Management VLAN • RMON – Statistic, History, Alarms, Events • Port Mirroring
7.	Ochrona przed atakami typu odmowa usługi	Przełącznik musi obsługiwać następujące funkcjonalności: • Ochrona CPU przed atakami Denial of Service (DoS)
8.	Protokoły ogólne	• Generic VLAN Registration Protocol (GVRP) • 802.1Q VLANs • 802.1D MAC Bridges • 802.1s Multiple Spanning Tree • 802.1t – Path Cost Amendment to 802.1D

		• 802.3ad Link Aggregation z 64 grupami na 8 portach • IP Multicast (IGMPv1,v2, v3) • Jumbo Packet ze wsparciem MTU Discovery Support dla interfejsu Gigabitowego (9216 bajtów) • Link Flap Detection • Dynamic Egress (Automatyczna konfiguracja portu VLAN) • 802.1ab LLDP-MED • Data Center Bridging: o 802.1Qaz o ETS (Enhanced Transmission Selection) o DCBx (Data Center Bridge Exchange Protocol) o 802.1Qbb PFC (Priority Flow Control) o 802,1Qau Congestion Notification • 802.3-2008 Clause 57 (Ethernet OAM – Link Layer OAM) • IGMP v1/v2/v3 Snooping oraz Querier • MLD IPv6 Snooping oraz Querier • QoS • RFC 3580 IEEE 802.1 RADIUS Usage Guidelines, z VLAN to Policy Mapping • Polityka musi obejmować jednocześnie ACL, QoS oraz przypisanie VLAN • Broadcast Suppression • ARP Storm Prevention • MAC-to-Port Locking • Span Guard (Spanning Tree Protection) • Algorytmy kolejkowania Strict Priority/ Weighted Round Robin • Obsługa min. 8 kolejek transmisyjnych na port • ToS/DSCP Marking/Remarking • 802.1p – Class of Service • 802.1D Priority-to-Transmit Queue Mapping • RFC 2865 RADIUS • FC 2866 RADIUS Accounting • TACACS+ • Standard MIB Support
9.	Uwierzytelnianie	• Obsługa uwierzytelniania: o 802.1X na porcie o przez sieć Web o wykorzystujące adres MAC • Obsługa wielu metod uwierzytelniania na jednym porcie, kolejność dowolnie konfigurowalna o Uwierzytelnianie wielu użytkowników/maszyn na jednym porcie, wraz z przypisaniem specyficznych polityk użytkownikowi/urządzeniu/maszynie wirtualnej o Jednoczesne uwierzytelnianie, co najmniej 100 użytkowników/maszyn końcowych (sesji uwierzytelniających) na port o Zależne od wyników uwierzytelniania przypisywanie sieci VLAN dla co najmniej 100 sieci VLAN 802.1Q (untagged egress) na port. • Zależne od wyników uwierzytelniania przypisywanie sieci VLAN dla co najmniej 100 sieci VLAN 802.1Q (ingress) na port.
10.	Dodatkowe	• Musi posiadać możliwość połączenia dwóch fizycznych urządzeń po przez łącza 40G tworząc jedno logiczne urządzenie(transmisja obustronna we wszystkich warstwach L2-L3-L4) • Wraz z przełącznikiem należy dostarczyć kable i przewody tego samego producenta, co dostarczane urządzenie do połączenia przełącznika z serwerem po przez łącza 2x10G RJ45. • Wraz z przełącznikiem należy dostarczyć kable i przewody tego samego

		producenta, co dostarczane urządzenie do połączenia urządzenia z siecią LAN po przez łącza 10x1G RJ45
11.	Gwarancja	Roczna gwarancja producenta, wymiana na następny dzień roboczy, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesje.
System sieci WLAN (punkty dostępowe) spełniające poniższe wymagania minimalne:		4 szt.
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Pasma robocze	Punkty dostępowe muszą obsługiwać równolegle dwa pasma częstotliwości 802.11a/n (5 GHz) i 802.11b/g/n (2.4 GHz).
2.	Radia	• dwa radia (a/n + b/g/n),
3.	Porty	• Wymagana minimalna ilość portów: 1 RJ-45 autosensing 10/100/1000 port (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex:10BASET/100BASE-TX: half or full; 1000BASE-T: full only, • Dedykowany port konsoli zarządzającej typu RJ-45,
4.	Standardy sieciowe	• Punkty dostępowe muszą być zgodne z DFS2 (Dynamic Frequency Selection) by dopuścić dodatkowe kanały w paśmie 5 GHz. • Kontrolery i punkty dostępowe muszą obsługiwać IP QoS w środowisku przewodowym i bezprzewodowym. Rozróżnianie pakietów musi być realizowane dla przychodzących i wychodzących pakietów z sieci bezprzewodowej, w oparciu o DiffServ, IP ToS oraz IP Precedence. • Punkty dostępowe muszą obsługiwać protokoły 802.11e, w tym WMM, TSPEC oraz U-APSD. • Musi obsługiwać szybki i bezpieczny roaming oraz handover (wstępne uwierzytelnienie, OKC). • Musi obsługiwać do 16 SSID (8 na częstotliwość radiową). • Musi obsługiwać RADIUS Authentication & Accounting. • Musi obsługiwać płynny roaming pomiędzy podsieciami IP. • Musi obsługiwać płynny roaming pomiędzy wieloma kontrolerami. • Wsparcie dla protokołu IEEE 802.1p prioritization, • AP powinien umożliwiać wykonanie minimum 12 jednoczesnych połączeń VoIP w ramach protokołu IEEE 802.11 a/b/g/n, • Punkty dostępowe powinny posiadać dwa radia zgodne z: IEEE 802.11/b/g/n oraz 802.11a/n, • Wymagane jest wsparcie dla protokołu: IEEE 802.1X z wykorzystaniem metod: EAP-SIM, EAPFAST, EAP-TLS, EAP-TTLS, and PEAP, • Wymagane jest wsparcie dla protokołu: MAC address authentication przy wykorzystaniu lokalnych access-list lub przesyłanych z serwera RADIUS, • Wymagane jest wsparcie dla mechanizmów: RADIUS AAA, przy wykorzystaniu EAP-MD5, PAP, CHAP oraz MS-CHAPv2, • Wymagane jest wsparcie dla mechanizmów: RADIUS Client • Wymagane jest wsparcie dla mechanizmów izolacji klientów na poziomie L2, • Wymagane jest wsparcie dla mechanizmów IEEE 802.11i, WPA2 oraz WPA, przy zastosowaniu algorytmów szyfracji: Advanced Encryption Standard (AES) oraz Temporal Key Integrity Protocol (TKIP), • Punkty dostępowe muszą obsługiwać technologię 802.11n pracując w konfiguracji 2x3 MIMO • Musi posiadać certyfikat 802.11n WiFi gwarantujący kompatybilność w sieciach WLAN • Musi mieć możliwość zapewnienia równego czasu antenowego (Airtime) dla wszystkich klientów w środowiskach, w których wspólnie występują technologie 802.11a/b/g oraz 802.11n
5.	Anteny	• Min. 4 anteny wewnętrzne,
6.	Tryby pracy	• Tryb działania radia WLAN: Client access, Local mesh, Packet capture, WDS • Możliwość pracy punktu dostępowego bez kontrolera WLAN na wypadek

		awarii łącza, • Punkty dostępowe muszą obsługiwać technologię 802.11n i pracę w technice transmisji wieloantenowej MIMO 2x2 przy zasilaniu przez jedno źródło zgodne z 802.3af, bez wpływu na działanie kluczowych funkcji i wydajności. • Wsparcie dla mechanizmu minimum „Two spatial stream MIMO" dla wszystkich nadajników • Punkty dostępowe muszą obsługiwać WDS (Wireless Distribution System) z możliwością tworzenia łączy typu backhaul na dowolnym łączu radiowym lub wykorzystania jednego łącza radiowego zarówno na potrzeby backhaul, jak i świadczenia usług klientom. • Punkt dostępowy musi obsługiwać instalację typu plug&play. • Punkty dostępowe muszą jednocześnie obsługiwać ruch tunelowany i mostowany. • Punkty dostępowe muszą mieć możliwość wdrożenia w formie sensorów sieci – pracujących w pełnym lub niepełnym wymiarze czasu. • W przypadku awarii punktu dostępowego, sąsiednie punkty dostępowe muszą rozszerzyć swój zasięg by wyeliminować niepokryte obszary, nawet w sytuacji, gdy punkt dostępowy nie może uzyskać dostępu do kontrolera. Wybór optymalnego kanału musi także być rekonfigurowany dynamicznie i bez interwencji użytkownika.
7.	Zarządzanie	• Punkt dostępowy musi zapewniać rozproszone zarządzanie łącznością radiową RF • Management (Radio Frequency), niezależne od kontrolera - poza tylko wstępną konfiguracją. Po utracie połączenia z kontrolerem, punkt dostępowy musi być zdolny do zapewnienia ciągłości operacji związanych z szyfrowaniem, tworzeniem czarnych list, filtrowaniem, QoS oraz zarządzaniem łącznością radiową, zarówno dla swoich potrzeb, jak i lokalnie mostowanego ruchu. • Zarządzanie łącznością radiową RF Management musi dostosowywać się do nowych kanałów w oparciu o wartości stosunku sygnału do szumu (SNR) i zajętości kanału, które mogą być ustalane przez użytkownika. • Punkty dostępowe sieci WLAN muszą mieć możliwość konfiguracji zapewniającej równoważenie obciążenia i sterowanie pasmem w celu pozwolenia punktom dostępowym na równoważenie/sterowanie ruchem klientów pomiędzy obiema częstotliwościami na jednym punkcie dostępowym i/lub pomiędzy wieloma punktami dostępowymi w ramach domeny łączności radiowej. • Punkty dostępowe muszą mieć możliwość wdrożenia w konfiguracji kratowej, tworzącej bezprzewodowe, wzajemne połączenia pomiędzy poszczególnymi punktami dostępowymi. • Możliwość stworzenia i jednoczesnego uruchomienia minimum 16 profili sieci bezprzewodowych WLAN, • Każdy profil wirtualny sieci bezprzewodowej powinien posiadać możliwość przypisania do VLAN'u,
8.	Bezpieczeństwo	• Połączenie pomiędzy AP, a kontrolerem musi być szyfrowane minimum AES 128 bit. • Punkty dostępowe muszą obsługiwać suplikanta 802.1x, by chronić swoje połączenia przewodowe przed nieautoryzowanym dostępem innych urządzeń. • Musi obsługiwać standardy uwierzytelniania i szyfrowania, w tym: WEP, WPA (TKIP), WPA2 (AES), 802.11i, 802.1x. • Punkt dostępowy musi wspierać szyfrowanie, tworzenie czarnych list, filtrowanie oraz QoS, niezależnie od kontrolera. • Musi obsługiwać funkcje egzekwowania polityk i ograniczania przepustowości w punkcie dostępowym. • Musi obsługiwać przypisywanie polityk klientom, bez konieczności segmentacji przez dedykowane SSID.

		• Musi wspierać polityki oparte na rolach zapewniające bezpieczeństwo, kontrolę dostępu i priorytety QoS, aplikowane względem użytkownika i aplikacji,
9.	WIPS	• wymagane jest scentralizowane raportowanie i konfiguracja WIPS/WIDS • Punkt dostępowy musi oferować funkcje WIPS/WIDS, działające bez wpływu na poziom świadczonych usług sieciowych, muszą być dostępne zarówno funkcje wykrywania, jak i zmniejszania zagrożeń, gdy punkt dostępowy świadczy innym klientom Wi-FI usługi transmisji danych Kategorie zagrożeń WIDS/WIPS, które należy wykrywać i raportować: • Analizy widma – zakłócenia pochodzące ze źródeł innych niż WiFi • Aktywna obserwacja – wykorzystanie narzędzi takich jak NetStumbler i Wellenreiter • Ataki typu chaff lub obfuskacja (tzw. zaciemnianie kodu) – ataki typu chaff mają za zadanie ukrywać obecności sieci, lub innych ataków na sieci • Atak Packet Injection (wtryskiwanie pakietów) – atakujący wprowadza swoje pakiety w transmisję danych pomiędzy dwoma urządzeniami, dzięki temu urządzenia traktują te złośliwe pakiety, tak jakby pochodziły z autoryzowanego urządzenia • Atak Denial of Service (skierowany na stację końcową) – zalewanie stacji końcowej komunikatami uwierzytelniania lub anulowania uwierzytelniania • Fałszywy klient (ang. Spoofing client) – urządzenie, które wykorzystuje adres MAC innej, zazwyczaj autoryzowanej stacji roboczej. Kategorie zagrożeń WIDS/WIPS, które należy wykrywać, raportować i zmniejszać: • Wewnętrzny Honeypot – punkt dostępowy rozgłaszający SSID, do którego nie ma upoważnienia • Zewnętrzny Honeypot – punkt dostępowy rozgłaszający SSID, którego nie oferuje dla danej usługi • Wrogi punkt dostępu (ang. Rogue AP) – punkt dostępowy podłączony do autoryzowanej sieci, pomimo braku upoważnienia do tego • Fałszywy punkt dostępu (ang. Spoofing AP) – urządzenie posługujące się BSSID (adres MAC) w rzeczywistości należącym do innego, autoryzowanego punktu dostępowego • Aktywne łamanie szyfrowania (ang. Active Encryption Cracking) – atak typu chop-chop i fragmentaryczny • Nieautoryzowane przekazywanie danych lub routing – urządzenie przekazuje pakiety pomiędzy sieciami, pomimo braku autoryzacji do tego procesu • Atak Denial of Service (skierowany na punkt dostępu) – zalewanie punktu dostępowego komunikatami autoryzacji i asocjacji.
10.	Dodatkowe	• Oprogramowanie działające na punktach dostępowych powinno umożliwiać oddzielną specyfikację częstotliwości dla każdego z modułów radia, Punkty dostępowe powinny posiadać certyfikację Wi-Fi Alliance, zapewniającą kompatybilną pracę z urządzeniami klienckimi w ramach standardu 802.11a/b/g/n, • Certyfikacja Wi-Fi Alliance Certification dla protokołów 802.11a/b/g/n,
11.	Gwarancja	Roczna gwarancja producenta, wymiana na następny dzień roboczy, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesje.
Rozwiązanie do zarządzania siecią spełniające poniższe wymagania minimalne:		1 szt.
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Funkcjonalność	• Musi zapewniać narzędzie do zarządzania na poziomie systemowym - umożliwiające implementacje dowolnej funkcjonalności wynikającej z karty katalogowej zarządzanego urządzenia • Musi umożliwiać centralne wykonywanie operacji systemowych, takich jak wykrywanie urządzeń, zarządzanie zdarzeniami, rejestrowanie zdarzeń i utrzymanie aplikacji

		• Musi zapewnić narzędzie umożliwiające szybkie i łatwe określenie fizycznej lokalizacji systemów i użytkowników końcowych oraz miejsca ich podłączenia do sieci • Musi zapewniać możliwości monitorowania całego systemu i wdrażania w nim konfiguracji VLAN • Musi zapewniać kompleksowe wsparcie zdalnego zarządzania dla wszystkich proponowanych urządzeń sieciowych, jak również wszystkich urządzeń zarządzanych przez SNMP MIB-I oraz MIB-II • Do obsługi zdalnej nie może wymagać stosowania żadnych klientów użytkowników końcowych lub oprogramowania typu agent • Musi umożliwiać śledzenie atrybutów urządzeń zainstalowanych w sieci, takich jak numer seryjny, etykieta zasobu, wersja oprogramowania *firmware*, typ CPU i pamięć
2.	Architektura	• Musi zapewniać scentralizowane zarządzanie urządzeniami sieci przewodowej i bezprzewodowej • Musi zawierać zintegrowane aplikacje typu *plug-in*, separujące poszczególne komponenty i uzupełniające możliwości systemu zarządzania. • Musi mieć możliwość instalacji, jako maszyna wirtualna • Musi obsługiwać możliwość automatycznego egzekwowania raz zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej ▪ Rozwiązanie musi integrować się ze środowiskiem wirtualnym: o Musi posiadać wsparcie dla VMware ESX i ESXi o Musi posiadać wsparcie dla Citrix XEN o Musi posiadać wsparcie dla Microsoft HyperV ▪ Obsługa funkcji wysokiej dostępności (High Availability
3.	Raportowanie	• Musi zapewniać możliwości modyfikacji, filtrowania i tworzenia własnych, elastycznych widoków sieci • Musi umożliwiać prezentowanie danych w formie wykresów lub tabelarycznej i pozwalać użytkownikowi na wybór wielu unikatowych identyfikatorów obiektów (*OID*) • Musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń) • Musi mieć możliwość generowania szczegółowego wykazu produktów zainstalowanych w sieci, zorganizowany według typu urządzenia • Musi rejestrować dane historyczne o atrybutach urządzenia i raportować jakiekolwiek zmiany w urządzeniu • Musi zapewniać dane historyczne o zmianach w konfiguracji i oprogramowaniu *firmware* urządzenia • Musi posiadać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania, spisem urządzeń • Musi umożliwiać generowanie szczegółowych raportów dla potrzeb związanych z planowaniem spisu urządzeń sieciowych • Musi zapewniać możliwości analiz na poziomie portu • Musi oferować możliwość tworzenia własnych, dostosowanych do potrzeb raportów przez tworzenie indywidualnych szablonów • Możliwość raportowania do elementu zarządzającego maszynami wirtualnymi (vSphere oraz XenCenter), informacji o rzeczywistym położeniu maszyny wirtualnej w sieci- fizyczny port i przełącznik
4.	Narzędzia administracyjne	• Musi pozwalać użytkownikowi na generowanie w tle zaplanowanych zdarzeń i zadań oraz planowanie terminu ich wykonania • Musi zapewnić narzędzie do podglądu i wyboru obiektów MIB *(Management Information Base)* z reprezentacji opartej na drzewie, oraz zawierać kompilator dla nowych lub pochodzących od innych dostawców MIB • Musi pozwalać administratorom IT na desygnowanie wybranego personelu do aktywowania/dezaktywowania wcześniej skonfigurowanych polityk w razie

		potrzeby • Musi umożliwiać prezentowanie szczegółowych informacji konfiguracyjnych, w tym datę i godzinę zapisów konfiguracji, wersję oprogramowania *firmware* i wielkość pliku konfiguracyjnego • Musi posiadać możliwość pobierania oprogramowania *firmware* do jednego urządzenia lub do wielu urządzeń jednocześnie • Musi mieć możliwość pobierania obrazów *boot PROM* do jednego urządzenia lub do wielu urządzeń jednocześnie • Musi posiadać zdolność do przeprowadzania zaplanowanych, rutynowych kopii zapasowych konfiguracji urządzeń • Musi mieć możliwość pobierania szablonów konfiguracyjnych w formacie tekstowym (ASCII) do jednego lub większej liczby urządzeń • Musi zapewniać interfejs sieci Web zawierający narzędzia do raportowania, monitorowania, rozwiązywania problemów i panele zarządzania • Musi zapewniać oparte o sieć Web elastyczne widoki, widoki urządzeń oraz dzienniki zdarzeń dla całej infrastruktury • Musi umożliwiać diagnozowanie problemów sieciowych i wydajności poprzez analizy danych NetFlow w czasie rzeczywistym
5.	Bezpieczeństwo	• Musi obsługiwać uwierzytelnianie RADIUS i LDAP dla użytkowników aplikacji • Musi obsługiwać bezpieczne zarządzanie przełącznikiem przez https. Musi mieć możliwość definiowania polityk: o ograniczających poziom pasma, o ograniczających liczbę nowych połączeń sieciowych, o ustalających pierwszeństwo ruchu w oparciu o mechanizmy QoS warstw 2 i 3, o nadających tagi pakietom, poddających kwarantannie poszczególne porty lub sieci VLAN i/lub uruchamiających wcześniej zdefiniowane działania • Musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej aplikacji, poprzez wykonanie jednej czynności, dzięki której polityki zostaną rozesłane do wszystkich urządzeń • Musi funkcjonować automatycznie gwarantując, że odpowiednie usługi są dostępne dla każdego użytkownika. Niezależnie od miejsca jego logowania do sieci • Musi współpracować z istniejącymi w danej sieci metodami uwierzytelniania, w szczególności z musi obsługiwać uwierzytelnianie oparte o 802.1X, Radius oraz MAC • Musi mieć możliwość natychmiastowego blokowania lub dopuszczania różnych aktywności sieciowych, w tym dostępu do sieci Web, poczty elektronicznej lub wymiany plików p2p • Musi zapewniać dynamiczne, konfigurowalne rozwiązanie powstrzymywania zagrożeń z szeroką gamą opcji reagowania, rejestrowania i audytowania • Musi natychmiastowo identyfikować fizyczną lokalizację i profil użytkownika źródła ataku • Musi mieć możliwość podejmowania działań w oparciu o wcześniej określone polityki bezpieczeństwa, włączając w to zdolność do powiadamiania systemu IDS o podjętych działaniach poprzez komunikat SNMPv3 *Trap* (*Inform*) • Musi umożliwiać automatyczne odłączanie lub izolowanie źródła nielegalnego lub nieodpowiedniego ruchu zidentyfikowanego przez system IDS
6.	Kontrola	• Musi zapewniać szczegółową kontrolę na poziomie portów, opartą na typie zagrożenia i zdarzenia • Musi zapewniać szczegółową kontrolę (każdego użytkownika i aplikacji) nad podejrzanymi działaniami i nieuprawnionym zachowaniem sieci

		• W przypadku spełnienia wcześniej określonych kryteriów musi mieć możliwość przypisania „roli kwarantanny" użytkownikowi podłączonemu do portu. • Musi umożliwiać izolowanie lub poddawanie kwarantannie atakującego, bez zakłócania pracy innych użytkowników, aplikacji lub systemów krytycznych dla danej organizacji • W przypadku spełnienia wcześniej określonych kryteriów musi dynamicznie odmawiać, ograniczać lub zmieniać parametry dostępu użytkownika do sieci • Możliwość przypisywania sieci VLAN, reguł filtrowania warstw L2-L4 oraz QoS na warstwach L2-L4 (DSCP i 802.1p) dla każdej maszyny wirtualnej opartej na przełączniku wirtualnym i wirtualnej grupie portów. Reguły filtrowania na warstwach L3-L4 i reguły QoS muszą obsługiwać zarówno IPv4, jak i IPv6.
7.	Wsparcie dla środowiska wirtualnego	• Możliwość konfiguracji vSwitch i PortGroups w ramach zarządzania maszynami wirtualnymi (vSphere i XenCenter), bez uruchamiania aplikacji do zarządzania maszynami wirtualnymi • Zdolność do ograniczania komunikacji pomiędzy maszynami wirtualnymi • Dostarczanie danych historycznych o obecności maszyny wirtualnej (na jakim rzeczywistym porcie oraz przełączniku, i w jakim czasie, dana maszyna wirtualna była obecna). • Dostarczanie informacji o systemie operacyjnym maszyny wirtualnej. • Możliwość dostarczenia informacji o stanie zabezpieczeń maszyny wirtualnej, po instalacji specjalnego modułu lub rozszerzeniu licencji. • Możliwość ograniczenia dostępu do określonych zasobów sieci, zgodnie z mechanizmem NAC, tylko dla zatwierdzonych maszyn wirtualnych. W przypadku przyłączenia maszyny wirtualnej do wirtualnej grupy portów lub wirtualnego przełącznika, ruch pochodzący z tej maszyny wirtualnej musi być blokowany, aż do momentu uzyskania odpowiednich praw dostępu dla tej maszyny wirtualnej. • Możliwość ograniczenia dostępu do określonych zasobów sieci zgodnie z mechanizmem NAC, także dla VDI (Virtual Desktop Infrastructure)
8.	Skalowalność	• Obsługa minimum 100 VM (Virtual Machine) jednocześnie, możliwość rozbudowy do obsługi 500 VM jednocześnie • Aplikacja musi umożliwiać przyszłą rozbudowę do minimum 500 urządzeń sieciowych oraz minimum 5000 punktów dostępowych
9.	Gwarancja	Roczna gwarancja producenta, wymiana na następny dzień roboczy, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesje.
Rozwiązanie kontroli dostępu do sieci dalej zwane NAC spełniające poniższe wymagania minimalne:		1 szt.
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Funkcjonalność	• Musi aktywnie zapobiegać przed dostępem do sieci nieautoryzowanych użytkowników, zagrożonych punktów końcowych i innych niechronionych systemów • Musi współpracować z rozwiązaniem Microsoft NAP • Rozwiązanie musi umożliwiać przypisanie na stałe adresu MAC do określonego przełącznika lub portu przełącznika. Jeżeli system końcowy będzie próbował się uwierzytelnić na innym porcie lub przełączniku, zostanie odrzucony lub przypisana mu zostanie polityka w oparciu o akcje określoną podczas przypisywania mu portu MAC • Musi posiadać funkcję *IP-to-ID Mapping*, która łączy razem nazwę użytkownika, adres IP, adres MAC oraz port fizyczny każdego punktu końcowego. Ta funkcjonalność jest kluczowa dla potrzeb audytów bezpieczeństwa i analiz dochodzeniowych • Musi także oferować zaawansowane możliwości przyznawania dostępu gościnnego takie jak: email oraz prosty portal służący do zatwierdzania

		rejestracji gości
2.	Architektura	▪ Musi zapewniać rozwiązanie NAC typu *inline* oraz *out-of-band*, które może być zarządzane przez jedną centralną aplikację ▪ Musi być dostarczone jako maszyna wirtualna pozwalając na wykorzystanie istniejącego sprzętu ▪ Musi mieć możliwość pracy jako redundantne urządzenia wirtualne w trybie wysokiej dostępności
3.	Raportowanie	• Rozwiązanie musi zapewniać informacje o typie urządzeń działających w sieci oraz określonych potrzebach i zagrożeniach, które są z nimi związane • Musi umożliwiać monitorowanie zdarzeń systemów końcowych i przedstawianie wyników o stanie zabezpieczeń systemu w oparciu o najbardziej aktualne skanowania przeprowadzane podczas oceniania • Musi posiadać możliwość szybkiego podglądu historycznych i ostatnich znanych stanów połączeń dla każdego systemu końcowego i uzyskiwać informacje o znalezionych podczas skanowania zagrożeniach bezpieczeństwa systemu końcowego • Musi zapewnić kompleksowe raportowanie zgodności w oparciu o aktualne i historyczne informacje • Musi obsługiwać powiadamianie poprzez syslog, pocztę elektroniczną lub usługi webowe o zmianach stanu systemów końcowych, rejestracji gości oraz wynikach skanowania stanu zabezpieczeń systemów końcowych
4.	Narzędzia administracyjne	• Musi zapewnić rozwiązanie oferujące jednolity, centralny obraz wszystkich niechronionych elementów związanych z użytkownikami i urządzeniami, który pozwoli później zredukować złożoność procesu zarządzania • Musi posiadać intuicyjny panel administracyjny, przedstawiający szczegółowy obraz stanu zabezpieczeń podłączonych lub próbujących się podłączyć systemów końcowych • Musi posiadać funkcję portalu rejestracyjnego dla kontroli dostępu gości, by zapewnić bezpieczne korzystanie z sieci przez gości, bez udziału pracowników działu IT.
5.	Bezpieczeństwo	• Rozwiązanie musi wykorzystywać oparte na standardach mechanizmy uwierzytelniania dla potrzeb procesów wykrywania, oceniania, kwarantanny, korygowania i autoryzacji podłączanych systemów końcowych • Rozwiązanie musi obsługiwać uwierzytelnianie RADIUS i/lub LDAP • Musi umożliwiać ciągłe mechanizmy analizowania zagrożeń, zapobiegania im i przechowywania ich • Rozwiązanie musi obsługiwać lokalną autoryzację MAC
6.	Kontrola	• Musi mieć zdolność ciągłego przypisywania polityk określonemu użytkownikowi, adresowi MAC lub OUI *(Organizationally Unique Identifier)* adresu MAC, tak aby użytkownik, urządzenie lub grupa urządzeń miały przydzielony ten sam zestaw zasobów sieci, niezależnie od swojej lokalizacji lub konfiguracji serwera RADIUS • Musi obsługiwać polityki umożliwiające przepuszczanie lub odrzucanie ruchu sieciowego, nadawanie mu priorytetów, ograniczanie jego szybkości, tagowanie, przekierowywanie i kontrolowanie go w oparciu o tożsamość użytkownika, czas i położenie, typ urządzenia i inne zmienne środowiskowe
7.	Wsparcie dla środowiska wirtualnego	• Możliwość objęcie mechanizmem NAC maszyn wirtualnych oraz VDI
8.	Automatyzacja	• Musi zapewniać automatyczne wykrywanie punktów końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, Kerberos) lub żądania RADIUS pochodzących z przełączników dostępowych
9.	Zgodność	• Powinien umożliwiać rozbudowę o możliwość oceniania w oparciu o agentów lub sieć (skanowania sieci) • Musi dostarczyć rozwiązanie, które zapewni ciągłość działania organizacji

		poprzez oferowanie użytkownikom alternatywnych metod dostępu podczas procesu skanowania • Musi przeprowadzać przed- i po-połączeniowe ocenianie stanu zabezpieczeń systemów końcowych
10.	Skalowalność	• Musi elastycznie obsługiwać wiele metod uwierzytelniania wielu użytkowników i urządzeń różnych dostawców • System musi umożliwiać kontrolę dla minimum 500 sesji autentykacyjnych • System musi umożliwiać przyszłą rozbudowę dla minimum 100 000 sesji autentykacyjnych
11.	Gwarancja	Roczna gwarancja producenta, wymiana na następny dzień roboczy, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesje.
Konfiguracja systemu i szkolenie		
1.	Zamawiający wymaga aby wymienione wyżej elementy Systemu bezprzewodowego i przewodowego zarządzania siecią zostały przez Wykonawcę zainstalowane oraz skonfigurowane. Wymaga się jednocześnie przeszkolenia minimum dwóch administratorów Zamawiającego w zakresie administracji i konfiguracji wyżej wymienionego systemu.	

X	**Licencje**	
Lp.	Nazwa komponentu	Ilość
1.	Windows Server Standard 2012 Government OPEN 1 License No Level 2 PROC	2 szt.
2.	VMware vSphere 5 Enterprise Plus Acceleration Kit for 6 processors	1 szt.
	Basic Support/Subscription VMware vSphere 5 Enterprise Plus Acceleration Kit for 6 processors	1 szt.
	Wymagania techniczne: - Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych. - Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. - Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone dowolną liczbę rdzeni oraz do 2TB pamięci fizycznej RAM. - Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-64 procesorowych. - Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 1 TB pamięci operacyjnej RAM. - Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć 1-10 wirtualnych kart sieciowych. - Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć co najmniej 4 porty szeregowe i 3 porty równoległe i 20 urządzeń USB. - Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. - Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. - Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Licencjonowanie nie może odbywać się w trybie OEM. - Rozwiązanie musi wspierać następujące systemy operacyjne: MS-DOS 6.22, Windows 3.1, Windows 95, Windows 98, Windows XP, Windows Vista , Windows NT 4.0, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, SLES 11, SLES 10, SLES 9, SLES 8, RHEL 6, RHEL 5, RHEL 4, RHEL 3, Solaris 11 ,Solaris 10, Solaris 9, Solaris 8, OS/2 Warp 4.0, NetWare 6.5, NetWare 6, NetWare 5, OEL 4, OEL 5, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu 12.04, SCO OpenServer, SCO Unixware, Mac OS X.	

	- Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. - Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. - Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno jako aplikacja na maszynie fizycznej lub wirtualnej jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. - Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. - Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. - Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. - Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. - Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. - Rozwiązanie musi zapewnić wbudowany mechanizm do bezpiecznej automatycznej archiwizacji i odtwarzania wskazanych maszyn wirtualnych. Mechanizm ten musi umożliwiać również odtwarzanie pojedynczych plików z kopii zapasowej oraz zapewnia stosowanie deduplikacji dla kopii zapasowych. - Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych. - Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie. - Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych w czasie ich pracy pomiędzy fizycznymi zasobami dyskowymi. - Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. - Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny które na nim pracowały były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. - System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów. - Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. - Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). - Rozwiązanie musi mieć możliwość automatycznego równoważenia obciążenia fizycznych zasobów dyskowych poprzez przenoszenie zwirtualizowanych dysków pracujących maszyn wirtualnych pomiędzy fizycznymi zasobami dyskowymi. Mechanizm ten musi być wyposażony w możliwość definiowania reguł przenoszenia np. przeniesienie zwirtualizowanych dysków maszyny wirtualnej wymusza przeniesienie zwirtualizowanych dysków innej lub zwirtualizowane dyski pojedynczej maszyny wirtualnej będą znajdowały się na tym samym lub różnych fizycznych zasobach dyskowych.

	- Oprogramowanie do wirtualizacji musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera a następnie wymuszać ten profil/konfigurację na innych serwerach lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym. - Rozwiązanie musi mieć możliwość zastosowania wirtualnych rozproszonych przełączników innych firm. Przełączniki te powinny posiadać możliwość ścisłej integracji z oprogramowaniem do wirtualizacji i być zaimplementowana jako wirtualne moduły liniowe na każdym hoście (serwerze) oraz redundantny moduł zarządzający. Implementacja stałego wirtualnego portu dołączającego maszynę wirtualną niezależnie od fizycznych serwerów (hostów) miedzy którymi maszyna jest migrowana. - Wirtualny przełącznik wbudowany w rozwiązanie lub firmy trzeciej musi posiadać następujące możliwości: • Agregacja portów: Możliwość agregacji indywidualnych portów na danym hoście (serwerze) do pojedynczej wiązki logicznej, zgodnie z protokołem LACP • QoS: Markowanie ruchu DSCP per wirtualny port; Dławienie (policing) ruchu per wirtualny port • Zarządzanie: Zarządzanie wirtualnym przełącznikiem złożonym z wirtualnych modułów liniowych znajdujących się w hostach (serwerach) z wykorzystaniem redundatnego wirtualnego modułu typu Supervisor; Implementacja Netflow lub podobnego mechanizmu dla statystyki ruchu; SNMP v3; Syslog Wymagane mechanizmy bezpieczeństwa: - bezpieczny dostęp w oparciu SSH; - Port Security dla wirtualnych portów dołączających wirtualne maszyny; - listy kontroli dostępu (ACL) na poziomie wirtualnych portów filtracja na poziomie warstw L2/L3/L4; - możliwość kopiowania ruchu z wybranego wirtualnego portu na inny określony wirtualny port na tym samym hoście (port monitorujący SPAN lub podobna funkcjonalność). - Możliwość kopiowania ruchu z wybranego wirtualnego portu i tunelowania go poprzez zewnętrzną sieć do urządzenia monitorującego (port ERSPAN lub podobna funkcjonalność); - Prywatne sieci VLAN; - Wsparcie dla RADIUS/TACACS+ W ramach dostawy oprogramowania, oferent jest zobowiązany do przeprowadzenia szkolenia dla minimum dwóch pracowników zamawiającego z zakresu instalacji, konfiguracji oraz zaawansowanej administracji dostarczonym oprogramowaniem.

XI	**Akcesoria**	
Lp.	Nazwa komponentu	Ilość
1.	Dyski SAS 2.0 2.5’’, kompatybilne z macierzą Fujitsu Eternus DX90 S2, o prędkości obrotowej 10 000 obr/min udostępniające użytkownikowi powierzchnie w trybie surowym min. 9TB.	14 szt.