AS/340/01/MM/2013

OPIS PRZEDMIOTU ZAMÓWIENIA

(minimalne wymogi, jakim ma odpowiadać przedmiot zamówienia)

Przetarg nieograniczony pt. „Dostawa urządzeń drukujących, materiałów eksploatacyjnych, oprogramowania i wyposażenia serwerowni dla Powiatowego Urzędu Pracy w Świebodzinie."

CZĘŚĆ I: Wyposażenie serwerowni:

1. *Przełącznik sieci LAN – 1 szt.*

- Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości 1U przystosowanym do montowania w szafie rack.
- Przełącznik musi posiadać 48 porty dostępowe Ethernet 10/100/1000 Auto-MDI/MDIX.
- Przełącznik musi być wyposażony w nie mniej niż 4 wbudowane porty uplink Gigabit Ethernet SFP– (obsługiwane co najmniej TX, SX, LX, LH, a także FX, BX-U i BX-D).
- Przełącznik musi posiadać zasilacz AC oraz moduł wentylacji. Musi istnieć możliwość podłączenia zewnętrznego redundantnego zasilacza AC.
- Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
- Przełącznik musi być wyposażony w nie mniej niż 1 GB pamięci Flash oraz 512 MB pamięci DRAM. Przełącznik musi posiadać slot USB pozwalający na podłączenie zewnętrznego nośnika danych. Przełącznik musi umożliwiać uruchomienie systemu operacyjnego z zewnętrznego nośnika danych umieszczonego w slocie USB.
- Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, ssh, a także za pośrednictwem interfejsu WWW.
- Przełącznik musi posiadać architekturę non-blocking. Wydajność przełączania w warstwie 2 nie może być niższa niż 56 Gb/s i 41 milionów pakietów na sekundę. Przełącznik nie może obsługiwać mniej niż 16 000 adresów MAC.
- Przełącznik musi obsługiwać ramki Jumbo (9216 bajtów).
- Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1Q w ilości nie mniejszej niż 1024. Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based).
- Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3AD - nie mniej niż 32 grupy LAG, po nie mniej niż 8 portów.
- Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spannig Tree, zgodnie z IEEE 802.1D-2004, a także Multiple Spanning Tree zgodnie z IEEE 802.1Q-2003 (nie mniej niż 64 instancje MSTP).
- Przełącznik musi obsługiwać protokół LLDP i LLDP-MED.
- Urządzenie musi obsługiwać ruting między sieciami VLAN – ruting statyczny, oraz protokół rutingu dynamicznego RIP. Ilość tras obsługiwanych sprzętowo nie może być mniejsza niż 6 000.
- Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności od co najmniej: interfejsu, typu

ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1P), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny.

- Urządzenie musi obsługiwać filtrowanie ruchu na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo nie mniej niż 1500 reguł filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu.
- Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, DHCP snooping.
- Przełącznik musi obsługiwać IEEE 802.1X zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przełącznik musi przypisywać ustawienia dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS (co najmniej VLAN oraz reguła filtrowania ruchu). Musi istnieć możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC. Przełącznik musi obsługiwać co najmniej następujące typy EAP: MD5, TLS, TTLS, PEAP.
- Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN.
- Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu rutingu IP, odpowiedzialnego za ustalanie tras rutingu i zarządzanie urządzeniem.
- Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 40 poprzednich, kompletnych konfiguracji.

2. Urządzenie firewall/VPN/UTM- 1 szt.

- Firewall musi być dostarczony jako dedykowane urządzenie sieciowe o wysokości **1 U**
- Urządzenie musi być wyposażone w co najmniej 1 GB pamięci RAM, pamięć Flash 1 GB oraz port konsoli. Urządzenie musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego firewalla z nośnika danych podłączonego do slotu USB na module kontrolnym.
- System operacyjny firewalla musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł rutingu IP, odpowiedzialny za ustalenie tras rutingu i zarządzanie urządzenia musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. System operacyjny firewalla musi śledzić stan sesji użytkowników (*stateful processing*), tworzyć i zarządzać tablicą stanu sesji. **Musi istnieć opcja przełączenia urządzenia w tryb pracy bez śledzenia stanu sesji użytkowników, jak również wyłączenia części ruchu ze śledzenia stanu sesji.**

- Urządzenie musi być wyposażone w nie mniej niż 2 wbudowanych interfejsy Ethernet 10/100/1000 oraz 6 wbudowanych interfejsów Fast Ethernet 10/100 (gotowych do użycia bez konieczności zakupu dodatkowych modułów i licencji).
- Urządzenie musi być wyposażone w 1 slot na dodatkowe karty z modułami interfejsów. Urządzenie musi obsługiwać co najmniej następującej rodzaje kart z modułami interfejsów: ADSL 2/2+, Serial, E1, Gigabit Ethernet (SFP). Urządzenia musi obsługiwać modem GSM podłączany do slotu USB lub slotu ExpressCard.
- Firewall musi realizować zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci oraz aplikacji pomiędzy nie mniej niż **12 strefami bezpieczeństwa** z wydajnością nie mniejszą niż **250 Mb/s** liczoną dla ruchu IMIX. Firewall musi przetworzyć nie mniej niż **90 000 pakietów/sekundę** (dla pakietów 64-bajtowych). Firewall musi obsłużyć nie mniej niż **32 000 równoległych sesji** oraz zestawić nie mniej niż **2 000 nowych połączeń/sekundę**.
- Firewall musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. IPSec VPN musi być realizowany sprzętowo. Firewall musi obsługiwać nie mniej niż **250** równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż **80 Mb/s**. **Urządzenie musi posiadać możliwość udostępniania użytkownikom wbudowanego klienta IPSec VPN za pośrednictwem strony WWW.**
- Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Firewall musi umożliwiać zdefiniowanie nie mniej niż **500** reguł polityki bepieczństwa.
- **Firewall musi posiadać możliwość** uruchomienia funkcji wykrywania i blokowania ataków intruzów (IPS, *intrusion prevention*) – mechanizm IPS musi być wspomagany sprzętowo. System zabezpieczeń musi identyfikować próby skanowania, penetracji i włamań, ataki typu exploit (poziomu sieci i aplikacji), ataki destrukcyjne i destabilizujące (D)DoS oraz inne techniki stosowane przez hakerów. Ustalenie blokowanych ataków (intruzów, robaków) musi odbywa się w regułach polityki bezpieczeństwa. System firewall musi realizować zadania IPS z wydajnością nie mniejszą niż **80 Mb/s**. Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia firewall. Baza sygnatur ataków musi być aktualizowana przez producenta codziennie.
- **Urządzenie zabezpieczeń musi posiadać możliwość uruchomienia wbudowanego modułu kontroli antywirusowej sprawdzającego pocztę elektroniczną (SMTP, POP3, IMAP), FTP oraz HTTP. Włączenie kontroli antywirusowej nie może wymaga dodatkowego serwera. Kontrola antywirusowa musi być wspomagana sprzętowo. Inspekcja antywirusowa musi być realizowana być realizowana z wydajnością na poziomie nie mniej niż 30 Mb/s dla ruchu HTTP. Musi istnieć możliwość wyboru działania mechanizmu kontroli antywirusowej w trybie sprzętowym i programowym.**
- **Urządzenie zabezpieczeń musi posiadać możliwość uruchomienia wbudowanego modułu kontroli antyspamowej działający w oparciu o mechanizm blacklist. Włączenie kontroli antyspamowej nie może wymaga dodatkowego serwera.**

- **Urządzenie zabezpieczeń musi posiadać możliwość uruchomienia wbudowanego modułu filtrowania stron WWW w zależności od kategorii treści stron. Włączenie filtrowania stron WWW nie może wymaga dodatkowego serwera.**
- **Urządzenie zabezpieczeń musi posiadać funkcję filtrowania zawartości ruchu HTTP, FTP i protokołów poczty elektronicznej (SMTP, POP3, IMAP) w celu blokowania potencjalnie szkodliwych obiektów. Urządzenie musi filtrować ruch na podstawie kryteriów obejmujących co najmniej: typy MIME, rozszerzenia plików, elementy ActiveX, Java i cookies.**
- Urządzenie musi obsługiwać protokoły dynamicznego rutingu: RIP, OSPF oraz BGP**. Urządzenie musi umożliwiać skonfigurowanie nie mniej niż 10 wirtualnych ruterów.**
- **Urządzenie musi posiadać możliwość uruchomienia funkcji MPLS z sygnalizacją LDP i RSVP w zakresie VPLS i L3 VPN.**
- **Urządzenie musi obsługiwać co najmniej 64 sieci VLAN z tagowaniem 802.1Q. W celu zapobiegania zapętlania się ruchu w warstwie 2 firewall musi obsługiwać protokoły Spanning Tree (802.1D) oraz Rapid STP (802.1W). Urządzenie musi obsługiwać protokół LACP w celu agregowania fizycznych połączeń Ethernet.**
- Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz obcinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych musi odbywa się na podstawie DSCP, IP ToS, 802.1p, oraz parametrów z nagłówków TCP i UDP. Urządzenie musi posiadać tworzenia osobnych kolejek dla różnych klas ruchu. Urządzenie musi posiada zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach.
- Firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie dla urządzeń zabezpieczeń Urządzenia zabezpieczeń w klastrze muszą funkcjonować w trybie Active-Passive z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze HA musi się odbywać przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
- Zarządzanie urządzeniem musi odbywać się za pomocą graficznej konsoli Web GUI oraz z wiersza linii poleceń (CLI) poprzez port szeregowy oraz protokoły telnet i SSH. Firewall musi posiadać możliwość zarządzania i monitorowania przez centralny system zarządzania i monitorowania pochodzący od tego samego producenta.
- Administratorzy muszą mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż **5** poprzednich, kompletnych konfiguracji.
- Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej przez okres 3 lat oraz aktualnej bazy sygnatur ataków, definicji wirusów, blacklist antyspamowych oraz bazy kategorii stron WWW przez okres 3 **lat**. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu, wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

3. Listwa dystrybucji zasilania- 2 szt.

Funkcja	Opis
Napięcie wyjściowe	200V, 208V, 230V
Gniazda wyjściowe	21 x IEC 320 C13 3 x IEC 320 C19
Maksymalne obciążenie	16A
Nominale napięcie wejściowe	200V, 208V, 230V
Częstotliwość na wejściu	50/60 Hz
Typ gniazda wejściowego	IEC-320 C20
Maksymalna wysokość	1791.00 mm
Maksymalna szerokość	56.00 mm
Maksymalna głębokość	46.00 mm
Możliwość zarządzania przez sieć	W pełni funkcjonalne sieciowe interfejsy zarządzania, które umożliwiają zarządzanie w oparciu o standardy WWW, SNMP i Telnet. Umożliwiają użytkownikom uzyskiwanie zdalnego dostępu do urządzeń, konfigurowanie ich i zarządzanie nimi, a tym samym zaoszczędzenie cennego czasu. Z możliwością tą wiąże się opcja szybkiego i łatwego aktualizowania oprogramowania firmware, które można pobrać z sieci do zainstalowanych urządzeń.
Zdalna kontrola pojedynczych wyjść	Zdalnie zarządza wyjściami, tak by użytkownicy mogli odłączyć wybrane, nie używane wyjścia (zapobiega przeciążeniu) lub przekierować zasilanie do zamkniętego sprzętu (minimalizuje kosztowne przestoje i eliminuje konieczność podejścia do sprzętu).
Lokalny wyświetlacz do monitorowania	Ogólny pobór mocy przez urządzenie rozdziału zasilania jest ukazany na wyświetlaczu urządzenia. Miejscowy wyświetlacz pomaga uniknąć przeciążenia obwodów, zapewniając wizualne ostrzeżenie w przypadku, gdy pobór prądu zbliża się do maksymalnego natężenia. (Dostępne tylko w oznaczonych SKU)
Opóźnienie zasilania	Umożliwia użytkownikom skonfigurowanie kolejności włączania i wyłączania zasilania w poszczególnych wyjściach. Pomaga to uniknąć kumulacji momentu rozruchowego przy starcie urządzeń, który może być przyczyną przeciążenia obwodu i odłączenie obciążeń. Ustalenie kolejności daje też użytkownikom możliwość ustalania kolejności włączania sprzętu, tak by inne zależne od niego urządzenia mogły działać prawidłowo.
Wskaźnik obciążenia LED	Informuje i przeciążeniu i warunkach zagrożenia na podstawie zdefiniowanych przez użytkownika progów alarmowych. Ostrzega użytkowników przez potencjalnym przeciążeniem obwodu.

Możliwość aktualizacji oprogramowania w pamięci flash	Szybko i prosto uaktualnij oprogramowanie sprzętowe pobierając je przez sieć. Eliminuje konieczność wymiany już zainstalowanych produktów, po ukazaniu się nowszych wersji. (Uwaga: tylko jednostki sieciowe)
Montowane w szafie	Obejmuje opcje montowane poziomo, pionowo i beznarzędziowo. Dostarcza zasilanie tam, gdzie jest ono najbardziej potrzebne - do szaf stojących obok sprzętu.
Interfejs użytkownika	Zgodny z posiadanymi listwami dystrybucji zasilania AP7921
Gwarancja	1 rok

4. System zasilania rezerwowego UPS-1 szt.

Funkcja	Opis
Moc wyjściowa	2700W / 3000 VA
Napięcie wyjściowe	230V
Informacja o napięciu wyjściowym	Możliwość konfiguracji znamionowego napięcia wyjściowego 220 /230/ 240
Częstotliwość na wyjściu (synchronicznie z siecią)	47–53 Hz przy częstotliwości nominalnej 50 Hz, 57–63 Hz przy częstotliwości nominalnej 60 Hz
Inne napięcia wyjściowe	220, 240
Topologia	Line Interactive
Typ przebiegu	sinusoida
Gniazda wyjściowe	8 x IEC 320 C13 1 x IEC 320 C19 3 x IEC Jumpers
Nominalne napięcie wejściowe	230V
Częstotliwość na wejściu	50/60 Hz +/-3 Hz (automatyczne wykrywanie)
Typ gniazda wejściowego	IEC-320 C20
Długość przewodu zasilania	2 metry
Zakres napięcia wejściowego w trybie podstawowym	160 - 286V
Zmienny zakres napięcia wejściowego w trybie podstawowym	151 - 302V
Inne napięcia wejściowe	220, 240
Typ akumulatora	Bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu szczelny
Typowy czas pełnego ładowania akumulatora	3 godziny
Port komunikacyjny	USB
Ilość interfejsów SmartSlot	1
Panel przedni	Wielofunkcyjna konsola sterownicza i informacyjna LCD
Alarm dźwiękowy	Alarm przy zasilaniu akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: konfigurowalne opóźnienia
Prognoza daty wymiany akumulatora	Dostarcza dynamicznie aktualizowanych

	informacji o zalecanym terminie wymiany akumulatorów (miesiąc i rok), wspomagając długoterminowe planowanie utrzymania infrastruktury.
Licznik energii	Informuje o rzeczywistej liczbie pobranych kilowatogodzin.
Powiadomienie o awarii akumulatora	Analiza uszkodzeń akumulatorów z funkcją wczesnego ostrzegania, co pozwala na podjęcie prewencyjnych czynności konserwacyjnych na czas
Kontrolki LED	W czytelny sposób informuje o jakości zasilania, stanie zasilacza UPS i akumulatora.
Możliwość zimnego startu	Tymczasowe zasilanie akumulatorowe w czasie zaniku zasilania sieciowego.
Akumulatory wymienialne przez użytkownika “na gorąco” bez przerywania pracy systemu	Zasilanie bezprzerwowe o znakomitych parametrach na czas operacji wymiany akumulatorów.
Powiadomienie o rozłączeniu akumulatora	Ostrzega, w przypadku gdy akumulator nie jest dostępny i nie może zapewnić zasilania awaryjnego.
Automatyczny test	Okresowy autotest akumulatora zapewnia wczesne wykrywanie konieczności wymiany.
Automatyczne włączenie UPS-a po powrocie zasilania	Automatycznie uruchamia podłączony sprzęt w momencie wznowienia zasilania z sieci miejskiej.
Maksymalna wysokość	86.00 mm
Maksymalna szerokość	480.00 mm
Maksymalna głębokość	683.00 mm
Wysokość w szafie przemysłowej	2 U
Wyposażenie dodatkowe	UPS należy wyposażyć w kartę do zarządzania o następujących parametrach: wsparcie dla protokołów komunikacyjnych (HTTP, HTTPS, IPv4, IPv6, NTP, SMTP, SNMP v1, SNMP v2c, SNMP v3, SSH V1, SSH V2, SSL, TCP/IP, Telnet), interfejs sieciowy RJ-45 10/100 Base-T , kompatybilność z UPSami z gniazdem SmartSlot, szyfrowanie kluczem o długości 2048, obsługa oprogramowania do zamykania systemów operacyjnych przez sieć LAN, wyposażona w czujnik pomiaru temperatury i wilgotności.
Gwarancja	1 rok

5. Szafa do zastosowań serwerowych i sieciowych wysokość 42U- 1 szt.

Szafa do zastosowań serwerowych i sieciowych wysokość 42U. Przystosowana do instalacji sprzętu 19" zgodnie ze standardem EIA-310-E

Cechy fizyczne
Maksymalna wysokość 199cm
Szerokość 75cm/60cm
Minimalna głębokość 107cm/120cm
Nośność minimalna 1300kg
Wysokość w szafie przemysłowej 42U
Minimalna głębokość montażu 26,2cm
Maksymalna głębokość montażu 91,5 cm
Kolor: czarny
Słupki pionowe– regulowana głębokość instalacji w szafie, otwory montażowe numerowany w pozycjach U
Drzwi przednie perforowane, zamykane na klamkę z kluczykiem
Możliwość zmiany drzwi przednich – prawe/ lewe
Drzwi tylne perforowane, dzielone, zamykane na klamkę z kluczykiem
Panele boczne
Szafa powinna być dostarczona w stanie złożonym
Dach, panele boczne oraz przednie i tylne drzwi powinny być uziemione do ramy obudowy. Na ramie powinno znajdować się osiem dodatkowych wkładek uziemiających służących do podłączania zewnętrznego uziemienia.
Kółka transportowe, nóżki poziomujące w miejscu docelowej instalacji,
Dostępny asortyment osprzętu montażowego - półki, prowadnice na kable, stabilizatory szafy
Okres gwarancji niemniej niż 5lata - naprawa lub wymiana
Osprzęt dodatkowy do szaf – w tym wentylatory dachowe
Szyny montażowe - Regulowana głębokość powinna umożliwić umieszczenie urządzenia w obudowie 19-calowej zgodnej z EIA-310-D.
Panele zaślepiające – instalowane bez narzędziowo, plastikowe panele 1U instalowane w nieużytkowanej przestrzeni szafy 19", minimum na 60U.

Dostawca musi przedłożyć potwierdzenie pochodzenia sprzętu z Autoryzowanego kanału dystrybucji Producenta/-ów.

CZĘŚĆ II: Serwer z macierzą dyskową:

1. Serwer- 1 szt.

Wysokość montażowa w szafie teleinformatycznej	2U
Procesory	Instalacja do maksymalnie dwóch 12-rdzeniowych procesorów Intel Xeon E5-2620 v2 Opis procesora: szybkość zegara min 2,0GHz, Max częstotliwość turbo 2,5 GHz, pamięć podręczna cache min 15MB, min 6 rdzeni, obudowa FC-LGA2011, szybkość, zestaw instrukcji 64-bit, znamionowa moc termiczna TDP 95W, mnożnik magistrali x25, technologia 32nm,

Pamięć podręczna procesora	Min 15MB na pojedynczy procesor
Pamięć RAM	Możliwość zainstalowania do 768 GB w 24 slotach. Zainstalowane min 96 GB w modułach o pojemnościach min 8GB.
Dyski twarde	Możliwość zainstalowania do 16 dysków HDD 2,5" lub 6 dysków HDD 3,5" lub 32 dysków SSD 1,8". Zainstalowane min 2 x HDD (pojemność: min 300GB, RPM: min 10K, Interfejs: SAS 6Gbps, typ: 2.5")
Kontroler RAID	Zintegrowany kontroler o przepustowości 6 Gbps wspierający pozimy RAID 0, 1, 10. Możliwość instalacji kontrolera o przepustowości 12 Gbps z poziomami RAID-0, 1, 10, 5, 50, 6, 60.
Zasilacze	Zainstalowane dwa redundantne zasilacze o mocy max 550W AC.
Interfejsy sieciowe LAN/SAN	Min 4 x 1Gb/s
Sloty rozszerzeń PCIe 3.0 (x16/x8)	4 lub 6 portów PCIe lub 4 porty PCI-X (CTO) lub 2 porty PCIe x16 (for GPU)
Porty USB	2 porty na panelu przednim 4 porty na panelu tylnym 2 porty wewnątrz obudowy
System zarządzania	IMM2, Diagnostyka optyczna LED wsparcie dla technologii Active Energy Manager
Systemy operacyjne	Wsparcie dla systemów operacyjnych: Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware vSphere
Gwarancja	3 lata gwarancji

2. ***Macierz dyskowa – 1 szt. wraz z dyskami- 6 szt. i kontrolerem- 1 szt.***

Lp.	Atrybut	Minimalne parametry techniczne
1	**Obudowa**	Możliwość instalacji do 12 dysków, rack 2U
2.	**Rozbudowa**	Możliwość rozbudowy infrastruktury do 192 dysków przez zakup dodatkowych półek dyskowych
3.	**Wentylatory**	Dostarczyć należy dwa moduły wentylatorów wymieniane podczas pracy serwera, każdy moduł posiada minimum dwa wentylatory
4.	**Zasilanie**	Dostarczyć należy zasilacze 2 x 500W działające w trybie redundantnym
5.	**Wyświetlacz**	LCM
6.	**Kontrolery**	Dostarczyć należy jeden kontroler sprzętowy. Obudowa musi posiadać możliwość dołożenia drugiego kontrolera
7.	**System plików**	ZFS
8.	**RAID**	Obsługa następujących poziomów RAID: 0,1,3,5,6,10,30,50,60. Globalny dysk zapasowy (hot spare), Dedykowany dysk zapasowy.
9.	**Cache kontrolera**	Dostarczany kontroler musi posiadać min 8 GB pamięci cache
10.	**Moduł BBM**	Dostarczyć należy moduł baterii w celu podtrzymania pamięci kontrolera

11.	**Dyski**	Dostarczyć należy min 6 dysków twardych o pojemności min 2TB każdy o parametrach 6Gb Sata 3,5”
12.	**Złącza**	7 x 1 Gb iSCSI
13.	**Funkcje**	Snapshot, SSD Caching, Volume Cloning, Zdalna replikacja, Thin Provisioning, deduplikacja (nie dotyczy iSCSI), UnifiedAUTH, migracja dysków on-line/off-line, RBAC (Role-Based Access Control), wsparcie dla QiSOE, Lista atrybutów S.M.A.R.T. dla SCSI, wsparcie dla Bootp
14.	**Szyny montażowe**	Dostarczyć należy szyny montażowe do instalacji w szafie 19” rack
15.	**Gwarancja**	3 lata
16.	**Produkt**	Fabrycznie nowy

CZĘŚĆ III: Oprogramowanie:

1. Oprogramowanie do wirtualizacji środowisk- 1 szt.

SYSTEM BEZ KONIECZNOŚCI ZAKUPU DODATKOWYCH LICENCJI MUSI:
- być instalowany bezpośrednio na serwerze fizycznym bez konieczności instalowania innego systemu operacyjnego (funkcja hypervisora);
-przechowywanie plików maszyn wirtualnych na własnym systemie plików.
-wsparcie dla technologii FibreChannel, iSCSI
-wsparcie dla technologii thin provisioning
-wsparcie dla różnych producentów systemów backupu
- umożliwiać wirtualizację na przynajmniej 3 serwerach 2-procesorowych;
- pozwalać na utworzenie maszyny wirtualnej zawierającej od 1 do 4 wirtualnych procesorów,
- ilość procesorów możliwych do przydzielenia maszynie wirtualnej nie większa niż 4 CPU;
- umożliwiać jednoczesną pracę wielu różnych maszyn wirtualnych (systemy operacyjne działające w nich aplikacje) na współdzielonych zasobach serwera;
- pozwalać na przenoszenie maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy aplikacji pracujących na maszynach wirtualnych;
- umożliwiać tworzenie klastrów z hostów fizycznych w celu zapewnienia wysokiej dostępności maszyn wirtualnych i aplikacji (ang. High Availability);
- posiadać zdolność do automatycznego ponownego uruchomienia maszyny wirtualnej przypadku jej awarii;
- umożliwiać wykonywanie kopii zapasowych i odtwarzanie z kopii zapasowej maszyn wirtualnych bez konieczności użycia agentów instalowanych na wirtualnych maszynach;
- pozwalać na wykonywanie wielu migawek stanu maszyn wirtualnych (snapshoot);
- umożliwiać przywracanie maszyny do każdego ze stanów utrwalonych przez przechowywane snapshooty;
- umożliwiać klonowanie/przenoszenie maszyn wirtualnych między serwerami infrastruktury bez potrzeby ich wyłączania;
- posiadać centralną konsolę graficzną do zarządzania wieloma maszynami wirtualnymi która musi: posiadać przynajmniej dwa interfejsy zarządzania; dedykowany klient i WWW; umożliwiać monitorowanie dostępności i wydajności maszyn wirtualnych; oferować dostęp do widoku topologii całego systemu i zbioru maszyn wirtualnych wraz z ich zasobami dyskowymi;
- umożliwiać automatyczne zarządzanie poprawkami dla infrastruktury;
- wspierać następujące systemy operacyjne: Windows 95, Windows 98, Windows 2000, Windows XP 32-bit, Windows XP 64-bit, Windows Vista 32-bit, Windows Vista 64-bit, Windows Serwer 2003 32-bit, Windows Serwer 2003 64-bit, Windows Serwer 2008 32- bit, Windows Serwer 2008 64-bit, FreeBSD7, Debian 5;
- nie zawierać ograniczenia ani na okres ważności licencji ani na okres używania oprogramowania;
- wsparcie dla skanowania ruchu maszyn wirtualnych z wykorzystaniem oprogramowania antywirusowego
- Wsparcie techniczne na okres 3 lat

2. ***Oprogramowanie do kompleksowego zarządzania siecią informatyczną- 1 szt.***

Opis wymagań (minimum)
Oprogramowanie powinno posiadać budowę modułową. Moduły powinny umożliwić kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. W zakresie obsługi sieci program powinien wykrywać konfigurację sieci automatycznie i pozwalać na jej prezentację na interaktywnych mapach. Monitorowanie infrastruktury powinno obejmować Serwery Windows, Linux, Unix, Mac; routery, przełączniki, VoIP, i firewall'e w zakresie: 1. Serwisów TCP/IP HTTP, POP3, SMTP, FTP i inne. Możliwość monitorować ich czasu odpowiedzi i procentu utraconych pakietów. 2. Serwerów pocztowych – Program powinien monitorować zarówno serwis odbierający, jak i wysyłający pocztę. – Program powinien mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia, w razie gdyby przestały one odpowiadać lub wadliwie funkcjonowały (np. gdy ważne parametry znajdą się poza zakresem). – Program powinien mieć możliwość wykonywania operacji testowych. – Program musi posiadać możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa. 3. Monitorowania serwerów WWW i adresów URL 4. Program powinien posiadać Inteligentne mapy i oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (mapy inteligentne). 5. Obsługa szyfrowania SSL w powiadomieniach e-mail 6. Urządzeń SNMP wspierających SNMP v1/2/3. Np: switch'e, routery, drukarki sieciowe, urządzenia VoIP itp. 7. Monitoringu routerów i przełączników wg: – Zmian statusu interfejsów sieciowych. – Ruchu sieciowego. – Podłączonych komputerów. – Generowanego ruchu przez podłączone komputery. 8. Serwisów Windows Monitor serwisów Windows powinien alarmować w razie gdy serwis przestanie działać oraz pozwalać na jego uruchomienie/zatrzymanie/zrestartowanie. 9. Wydajności systemów Windows Obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy. <u>W zakresie inwentaryzacji sprzętu program powinien automatycznie gromadzić informacje o sprzęcie i oprogramowaniu urządzeń w sieci oraz:</u> 1. Prezentować szczegóły dotyczące sprzętu: model, CPU, pamięci, płyty głównej, napędów, kart, etc. 2. Audyt sprzętowy powinien obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dysku, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. 3. Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w firmie. 4. Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranym komputerze: instalacji/deinstalacji aplikacji, zmian adresu IP itd.

Opis wymagań (minimum)

5. Posiadać możliwość wysyłania powiadomienia np. emialem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
6. Umożliwić odczytywania numeru seryjnego (klucze licencyjne).

Z modułem inwentaryzacji sprzętu program powinien umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie:

1. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
2. definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania powinna istnieć możliwość podawania dodatkowych informacji, np. **numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin przeglądu** (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny plik .DOC, .XLS, skan dokumentu czy też własny komentarz; możliwość importu danych z zewnętrznego źródła (CSV),
3. możliwości wygenerowania zestawienia wszystkie środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania.
4. możliwość archiwizacji i porównywania audytów środków trwałych
5. **Kody kreskowe w Środkach Trwałych-** możliwość drukowania kodów kreskowych oraz QR Code (mozaikowe) dla środków trwałych, które posiadają numer inwentarzowy dzięki aplikacji mobilnej na android, można inwentaryzować sprzęt posiadający kody kreskowe.

Inwentaryzacja oprogramowania powinna zapewnić funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:

1. Skanowanie plików wykonywalnych i multimedialnych na dyskach komputerów oraz skanowanie archiwów.
2. Zarządzanie posiadanymi licencjami; pakietami oprogramowania, licencjami dostępowymi (tzw. CAL'e) itd.
3. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili powinna istnieć możliwość wykonania aktualnych raportów audytowych.
4. Zarządzanie posiadanymi licencjami: raport zgodności licencji
5. Możliwość przypisania do programów numerów seryjnych, wartości itp.

Okna audytowe posiadają możliwość filtrowania elementów per oddział
W zakresie obsługi użytkowników program powinien umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez analizę:

1. Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy).
2. Monitorowanie procesów (każdy proces ma całkowity czas działania oraz czas wykorzystania przez użytkownika)
3. Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona),
4. Informacji o edytowanych przez pracownika dokumentach.
5. Historii pracy (cykliczne zrzuty ekranowe)
6. Listy odwiedzanych stron www (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt)
7. Transferu sieciowego użytkowników **(**ruch sieciowy lokalny i transfer internetowy wygenerowany przez pracowników)
8. Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, zestawienia pod względem użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukował), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację

Opis wymagań (minimum)
drukarek. Program będzie miał możliwość monitorowania kosztów wydruków. Program ponadto powinien posiadać możliwość blokowanie stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla danego użytkownika z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danej strony. Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. Mechanizm blokowania uruchamiania aplikacji. Kolejny moduł powinien umożliwiać realizację zdalnej pomocy użytkownikom sieci lokalnej. W ramach kontroli stacji użytkownika wymagany jest podgląd pulpitu użytkownika i możliwość przejęcia jego konsoli. Ważne aby podczas przejęcia kontroli nad komputerem pracownika zarówno pracownik jak i administrator widzieli ten sam ekran. W powyższym module powinna znajdować się baza zgłoszeń umożliwiająca użytkownikom zgłaszać problemy techniczne, które z kolei byłyby przetwarzane i przyporządkowywane odpowiednim administratorom (wg kategorii problemów) otrzymującym automatycznie powiadomienie o przypisanym im problemie do rozwiązania. Atutem będzie funkcjonalność pozwalająca użytkownikom na monitorowanie procesu rozwiązywania zgłoszonego przez niego problemu i jego aktualnego statusu, jak również wymiany informacji z administratorem za pomocą komentarzy, które mogą być wpisywane i śledzone przez obydwie strony. Moduł ten powinien zawierać również komunikator **(czat)** który umożliwiać będzie przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami. W module tym powinna być możliwość pobrania użytkowników z Active Directory Obsługa załączników w module HelpDesk Obsługa zrzutów ekranowych w module HelpDesk Dystrybucja oprogramowania przez Agenty: Dystrybucja oraz uruchamianie plików za pomocą Agentów (w tym plików MSI); Mechanizm kolejkowania dystrybucji, jeśli komputer jest wyłączony w trakcie zlecania operacji Kolejny moduł programu powinien posiadać w sobie możliwość ochrony danych przed wyciekiem przez blokowanie urządzeń **1. Blokowanie urządzeń i nośników danych** Program, ma możliwość zarządza prawami dostępu do wszystkich urządzeń wejścia i wyjścia (przewodowych i bezprzewodowych) oraz urządzeń fizycznych, przez które użytkownik może skopiować pliki z komputera firmowego lub uruchomić na nim program zewnętrzny. 1. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda SD itp., SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek 2. Blokowanie interfejsów bezprzewodowych: WiFi, Bluetooth, IrDA 3. Blokada dotyczy tylko urządzeń do przenoszenia danych - inne urządzenia (drukarka, klawiatura itp.) można podłączyć **<u>Zarządzanie prawami dostępu do urządzeń</u>** 1. Definiowanie praw użytkowników/grup do odczytu i kopiowania plików 2. Autoryzowanie urządzeń firmowych: pendrive'ów, dysków itp. - urządzenia prywatne są blokowane 3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników lub komputerów 4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci lub wybranych grup

Opis wymagań (minimum)
komputerów **Audyt operacji na urządzeniach przenośnych** 1. Zapisywanie informacji o operacjach zapisu w systemie plików na urządzeniach przenośnych 2. podłączenie/odłączenie pendrive'a 3. Zapisywanie informacji o operacjach zapisu w systemie plików na urządzeniach przenośnych **Integracja modułu z Active Directory** - zarządzanie prawami dostępu przypisanymi do użytkowników **Ochrona przed usunięciem** Program jest zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora. Program powinien zawierać minimum 12 miesięcy pomocy technicznej oraz aktualizacji. Program powinien być w języku polskim

3. System kopii zapasowych- 1 szt.

I. Założenia ogólne:

1. System kopii zapasowych ma opierać się o architekturę klient-serwer, z centralnym serwerem zarządzającym procesem backupu oraz klientami (agentami) instalowanymi na maszynach w sieci.
2. System kopii zapasowych ma umożliwiać prostą promocję każdego z klientów (niezależnie od wykorzystywanego systemu operacyjnego) zarejestrowanych w centralnym systemie backupu do funkcji serwera mediów, który może posłużyć do składowania backupu z innych klientów.
3. Powyższa funkcja ma umożliwiać promocję klienta do funkcji serwera mediów z wykorzystaniem dedykowanej funkcji interfejsu Web, w szczególności niedopuszczalne jest, aby konieczne było modyfikowanie plików konfiguracyjnych klienta oraz serwera a także konieczność zmian na samym kliencie.
4. Funkcja serwera mediów ma umożliwiać wykorzystanie zarówno lokalnych zasobów dyskowych każdego z klientów, jak również napędu taśmowego oraz biblioteki taśmowej do nich podłączonych celem zapisania na nich backupu z pozostałych klientów.
5. Jedynym ograniczeniem skorzystania z funkcjonalności promocji klienta do roli serwera mediów może być licencja.
6. System kopii zapasowych ma mieć możliwość wykonywania backupu na dysk, na taśmę (z wykorzystaniem napędu taśmowego oraz biblioteki taśmowej) a także do chmury utworzonej z serwerów backupu zainstalowanych w zdalnych lokalizacjach.
7. System backupu ma posiadać możliwość backupu 1TB danych w podstawowej licencji (z możliwością rozbudowy).
8. System ma być wyposażony w mechanizm deduplikacji, który pozwoli zaoszczędzić ilość miejsca na dysku poprzez wyszukiwanie bloków zapisanych na nośniku w poprzednim zadaniu backupu.
9. System ma być wyposażony w licencję, która gwarantuje współpracę z bibliotekami taśmowymi z wbudowanymi mechanizmami robotyki, bez względu na liczbę kaset oraz napędów obsługiwanych przez daną bibliotekę.
10. System ma mieć możliwość obsługi nielimitowanej ilości napędów i bibliotek taśmowych.
11. System ma mieć możliwość autodetekcji dowolnego napędu taśmowego i biblioteki, która została do niego podłączona.

12. Administrator ma mieć możliwość ręcznej definicji dowolnego napędu taśmowego i biblioteki wraz z informacjami dotyczącymi jego budowy.
13. System ma być wyposażony w moduł zarządzania licencjami, gdzie poprzez interfejs Web, administrator ma możliwość dodawania dowolnej licencji.
14. Moduł zarządzania licencjami ma mieć możliwość dodawania (rozbudowy) poszczególnych funkcjonalności oprogramowania bez konieczności uruchamiania ponownie żadnego z komponentów oprogramowania. Niedopuszczalna jest konieczność restartu jakichkolwiek usług wchodzących w skład oprogramowania oraz jakichkolwiek maszyn wchodzących w skład systemu kopii bezpieczeństwa (włączając w to maszyny z zainstalowaną aplikacją klienta).
15. System backupu musi mieć możliwość obsługi nielimitowanej ilości klientów backupu, wliczając w to agentów systemu plików oraz agentów dla hypervisorów (VMware, Hyper-V).

II. Centralny serwer backupu:

1. Centralny serwer backupu ma mieć możliwość instalacji na dowolnym systemie Linux. Niedopuszczalne jest, aby produkt wymagał instalacji na konkretnych, komercyjnych systemach Linux a także na dedykowanych systemach operacyjnych producenta danego rozwiązania.
2. Niedopuszczalne jest, aby serwer backupu musiał być instalowany na innych systemach niż system Linux, w szczególności niedopuszczalne jest wykorzystanie systemów z rodziny Windows oraz Mac.
3. Instalator centralnego serwera backupu ma być dostarczony w formie instalatorów dla poszczególnych rodzin systemu Linux, minimum jako: pakiet RPM (dla systemów zgodnych z Red Hat), pakiet DEB (dla systemów zgodnych z Debian) oraz jako archiwum tar.gz dla pozostałych.
4. Interfejs zarządzania serwerem backupu ma być dostępny poprzez przeglądarkę internetową.
5. Wspierane przez producenta przeglądarki do zarządzania serwerem backupu to minimum Mozilla Firefox 3.0 lub nowszy oraz Microsoft Internet Explorer 7.0 lub nowszy.
6. Funkcjonalność zarządzania programem przez przeglądarkę ma być dostępna jako funkcja dodatkowa i ma być dostępna do pobrania z serwerów producenta w postaci odrębnego instalatora.
7. Instalator systemu zarządzania poprzez przeglądarkę ma być dostarczony w formie instalatorów dla poszczególnych rodzin systemu Linux, minimum jako: pakiet RPM (dla systemów zgodnych z Red Hat), pakiet DEB (dla systemów zgodnych z Debian) oraz jako archiwum tar.gz dla pozostałych.
8. Interfejs systemu ma być dostępny przez przeglądarkę za pomocą protokołu HTTPS, tym samym cała komunikacja pomiędzy przeglądarką a systemem ma być szyfrowana.
9. W domyślnej konfiguracji, interfejs dostępny przez przeglądarkę nie ma wykorzystywać portów TCP niższych niż 1024, w szczególności niedopuszczalne jest, aby interfejs nasłuchiwał na portach 80 oraz 443.
10. Administrator ma mieć możliwość zdefiniowania dowolnego portu TCP, na którym nasłuchiwać będzie interfejs dostępny poprzez przeglądarkę.
11. W domyślnej konfiguracji programu, autoryzacja do systemu zarządzania ma być możliwa z konta użytkownika Root, gdzie hasło ma być puste.
12. System ma umożliwiać utworzenie dowolnej ilości kont użytkowników.
13. Użytkownicy w systemie muszą mieć możliwość przypisania roli odzwierciedlającej poziom uprawnień.
14. W domyślnej konfiguracji, system ma oferować minimum 3 rodzaje kont użytkowników systemu:
    a) Administrator - może wykonywać wszystkie typy operacji w systemie w tym tworzyć, modyfikować oraz usuwać obiekty i konta użytkowników,
    b) Operator – może uruchamiać zadania backupu, ma dostęp z uprawnieniami tylko do odczytu do konfiguracji systemu,
    c) Użytkownik – nie może tworzyć, usuwać ani modyfikować jakichkolwiek obiektów w systemie, ma prawo jedynie do odtwarzania kopii zapasowych.
15. Serwer backupu ma umożliwiać dwukierunkową komunikację z agentami.
16. Serwer backupu ma mieć możliwość połączenia z agentem zarówno za pomocą adresu IP jak również z wykorzystaniem nazwy DNS.
17. Produkt ma posiadać możliwość replikacji danych pomiędzy wieloma serwerami backupu zlokalizowanymi w różnych, także odległych lokalizacjach za pośrednictwem sieci LAN oraz łącz WAN.

18. Proces replikacji danych pomiędzy serwerami backupu ma mieć możliwość definiowania minimum takich właściwości jak:
    a) dane przeznaczone do replikacji z dokładnością do pojedynczego zasobu dyskowego,
    b) częstotliwość z jaką replikacja będzie się odbywać z dokładnością do minuty, momentu zakończenia replikacji (musi być możliwość zdefiniowania daty końcowej, wyłączenia daty końcowej – replikacja ciągła oraz zdefiniowania ilości wystąpień zadania replikacji, po których polityka przestanie być aktywna),
    c) retencji z dokładnością do jednego dnia.
19. Produkt ma posiadać możliwość replikacji danych pomiędzy lokalnymi zasobami dyskowymi, tym samym administrator ma mieć możliwość zwielokrotnienia tych samych danych na wielu zasobach dyskowych celem zabezpieczenia danych przed awarią pojedynczego zasobu dyskowego.
20. Proces replikacji danych pomiędzy lokalnymi zasobami dyskowymi ma być wyzwalany na żądanie administratora. Administrator ma być w stanie określić przed rozpoczęciem replikacji:
    a) źródłowy logiczny zbiór danych do replikacji (z dokładnością do pojedynczego pliku),
    b) docelowy zasób dyskowy, na który dane mają zostać zreplikowane,
    c) czas retencji dla danych replikowanych.
    d) włączenie/wyłączenie raportowania na e-mail o szczegółach wykonania zadania replikacji,
    e) wyłączenie aktualizacji indeksu danych o dane zreplikowane
    f) ustawienie limitu czasowego po przekroczeniu, którego proces replikacji zostanie zatrzymany.
21. System ma umożliwiać prostą rozbudowę o opcję związaną z szyfrowaniem backupu z wykorzystaniem przynajmniej takich algorytmów jak 3DES (z PCBC), Blowfish oraz AES256 za pomocą pojedynczego pliku licencji instalowanej na serwerze backupu.
22. Klucze szyfrujące nie mogą być zapisywane razem z danymi backupowanymi.
23. Klucze mają być przechowywane na kliencie (agencie) a nie na centralnym serwerze backupu.
24. Funkcjonalność szyfrowania danych ma zabezpieczać zarówno dane przesyłane przez sieć jak również dane zapisywane na centralnym serwerze backupu.
25. Serwer backupu ma mieć możliwość definiowania parelizmu (maksymalnej wartości jednoczesnych operacji) dla zasobu dyskowego, przy czym wartość maksymalna nie ma być niższa niż 15.
26. System ma oferować możliwość odtwarzania backupu z możliwością określenia:
    a) czy odtworzone mają być oryginalne prawa na plikach,
    b) daty modyfikacji,
    c) ACL w systemie POSIX oraz atrybutów rozszerzonych Linux,
    d) czy nadpisywać pliki, jeśli istnieją na docelowej maszynie,
    e) czy nadpisywać pliki, jeśli są nowsze niż te, które znajdują się w backupie.
27. Podczas odtwarzania, administrator ma ponadto mieć możliwość zdefiniowania systemu innego niż centralny system backupu, który będzie źródłem dla procesu odtwarzania.
28. System ma oferować możliwość kompresji danych backupu przed przesłaniem ich poprzez sieć na backup serwer, możliwość ta ma istnieć jako opcja dla każdego z definiowanych zadań backupu.
29. Algorytm kompresji wykorzystywany do kompresji backupu ma bazować na algorytmie LZ77, w szczególności niedopuszczalne jest stosowanie zamkniętych algorytmów kompresji danych.
30. Centralny serwer backupu ma być wyposażony w mechanizm reindeksacji istniejących taśm z backupem. W przypadku uszkodzenia indeksu, funkcja ta musi mieć możliwość zaindeksowania taśm utworzonych zarówno na danym centralnym serwerze backupu, jak i na każdym innym centralnym serwerze backupu wchodzącym w skład środowiska backupu.
31. Mechanizm reindeksacji taśm ma umożliwiać administratorowi określenie następujących właściwości procesu przed jego rozpoczęciem:
    a) w przypadku znanych taśm: wybór źródłowej taśmy, wybór źródłowego napędu, wybór czy rozpocząć indeksację od momentu jej przerwania czy od początku nośnika, wybór czy wysunąć taśmę z napędu po zakończeniu procesu indeksacji oraz czy po zakończeniu procesu przesłać powiadomienie do administratora drogą elektroniczną z podsumowaniem procesu indeksacji,
    b) W przypadku nieznanych taśm: wybór źródłowego napędu, wybór puli taśmowej do podłączenia, wybór typu taśmy – produkt ma zawierać listę minimum 76 predefiniowanych typów taśm (w tym

minimum ma oferować taśmę typu NULL oraz FILE celem testowania poprawności konfiguracji), zdefiniowania czy w zadaniu użyta ma być biblioteka taśmowa (jeśli tak, administrator ma mieć opcję wskazania której biblioteki należy użyć podczas procesu reindeksacji oraz którego slotu tej biblioteki), wybór czy rozpocząć indeksację od momentu jej przerwania czy od początku nośnika, wybór czy wysunąć taśmę z napędu po zakończeniu procesu indeksacji oraz czy po zakończeniu procesu powiadomić administratora wiadomością e-mail z podsumowaniem procesu indeksacji.

32. Centralny serwer backupu ma być wyposażony w mechanizm reindeksacji istniejących zasobów dyskowych z backupem w przypadku uszkodzenia indeksu. Funkcja ta ma mieć możliwość zaindeksowania dysków z danymi zarówno na danym centralnym serwerze backupu, jak i na każdym innym centralnym serwerze backupu wchodzącym w skład środowiska backupu.
33. Mechanizm reindeksacji dysków ma umożliwiać administratorowi określenie takich właściwości procesu przed jego rozpoczęciem jak:
    a) w przypadku znanych dysków: wybór źródłowego zasobu dyskowego, wybór czy rozpocząć indeksację od momentu jej przerwania czy od początku nośnika oraz czy po zakończeniu procesu przesłać powiadomienie do administratora drogą elektroniczną z podsumowaniem procesu indeksacji,
    b) w przypadku nieznanych dysków: wybór hosta należącego do systemu backupu, do którego podłączony jest zasób dyskowy, definicja nazwy dla nowoutworzonego zasobu dyskowego po indeksacji, wskazanie pełnej ścieżki do indeksowanych danych, zdefiniowanie wielkości wolumenu z dokładnością do 1 megabajta, wybór czy rozpocząć indeksację od momentu jej przerwania czy od początku nośnika oraz czy po zakończeniu procesu przesłać powiadomienie do administratora drogą elektroniczną z podsumowaniem procesu indeksacji.
34. System ma być wyposażony w mechanizm weryfikacji taśm, który umożliwia test czy dane zapisane na taśmie mogą być poprawnie odczytane.
35. Powyższa funkcjonalność ma umożliwiać administratorowi zdefiniowanie przed rozpoczęciem procesu weryfikacji minimum następujących elementów:
    a) wybór taśmy do weryfikacji,
    b) wybór napędu, który posłuży do weryfikacji,
    c) wybór czy wznowić weryfikację od momentu, w którym proces został przerwany,
    d) wybór czy wysunąć taśmę z napędu po zakończeniu procesu weryfikacji
    e) czy po zakończeniu procesu przesłać powiadomienie do administratora drogą elektroniczną z podsumowaniem procesu weryfikacji.
36. System ma być wyposażony w mechanizm duplikacji taśm z zapisanymi na nich kopiami bezpieczeństwa, który umożliwi utworzenie dowolnej ilości kopii danej taśmy celem zabezpieczenia danych przed awarią lub zniszczeniem nośnika.
37. Powyższa funkcjonalność ma umożliwiać administratorowi zdefiniowanie przed rozpoczęciem procesu duplikacji minimum następujących elementów:
    a) wybór źródłowej taśmy z danymi do duplikacji,
    b) wybór napędu, w którym umieszczono źródłową taśmę,
    c) wybór napędu, w którym umieszczono taśmę docelową,
    d) możliwość wyboru czy podczas procesu będzie wykorzystywana biblioteka taśmowa (jeśli tak, to dodatkowo administrator ma mieć możliwość zdefiniowania, której biblioteki należy użyć podczas procesu oraz slotu w którym zainstalowano taśmę docelową),
    e) możliwość wymuszenia nadpisywania danych na taśmie docelowej,
    f) czy po zakończeniu procesu przesłać powiadomienie do administratora drogą elektroniczną z podsumowaniem procesu duplikacji.
38. System ma być wyposażony w mechanizm nawigacji, który umożliwia przeglądanie przez przeglądarkę Web zawartości dysków twardych wszystkich klientów zarejestrowanych w centralnym serwerze backupu oraz dodatkowo jego własne dane. Dane mają być wyświetlane w formie drzewa katalogów z możliwością przeglądania ich zawartości.
39. Powyższa funkcjonalność ma działać niezależnie od systemu operacyjnego klienta oraz serwera. W każdym przypadku administrator ma mieć możliwość przeglądania plików i katalogów oraz weryfikacji poprawności komunikacji pomiędzy klientem a serwerem.

40. Mechanizm nawigacji ma oferować możliwość weryfikacji, czy na stacji poprawnie zainstalowano agenta do hot-backupu aplikacji (agent ma wówczas w drzewie przypisanym do danego klienta wyświetlać listę takich aplikacji).
41. System ma być wyposażony w mechanizm automatycznego wykrywania urządzeń takich jak napędy i biblioteki taśmowe, które zostały podłączone do centralnego systemu backupu.
42. Powyższa funkcja nie może wymagać od administratora uprzedniej instalacji sterowników do obsługi danego urządzenia.

III. Agent do backupu środowiska wirtualnego VMware vSphere:

1. Agent backupu ma wspierać hot-backup (backup w czasie pracy) dla platformy wirtualizacyjnej VMware Infrastructure w wersjach ESX 3.0, 3.5, ESXi 3.x, Virtual Center 2.0, 2.5.
2. Agent backupu ma wspierać hot-backup (backup w czasie pracy) dla platformy wirtualizacyjnej VMware **vSphere w wersjach** ESXi 4.x, 5.0, ESX 4.x, vCenter 4.0, 4.1, 5.
3. Agent backupu ma wspierać obsługę środowiska wirtualizacji vStorage na platformach CentOS 5, Red Hat Enterprise Linux 5, 6, SUSE Enterprise Server 10, 11, Windows Server 2003 SP2, Windows Server 2008 SP1 and R2, Windows Desktop: 7, Vista, XP SP3.
4. Funkcjonalność agenta backupu ma umożliwiać backup zarówno zatrzymanych jak również pracujących maszyn wirtualnych bez konieczności instalacji agenta na każdej z tych maszyn (backup na poziomie hypervisora).
5. Backup ma być możliwy zarówno dla całych obrazów maszyn wirtualnych, jak i na poziomie poszczególnych wykorzystanych bloków.
6. Backup ma być realizowany jako backup pełny, jako backup przyrostowy i dyferencyjny na poziomie bloków.
7. Agent backupu ma umożliwiać backup tylko danych fizycznie zapisanych na wirtualnym dysku.
8. Agent backupu ma zapewniać możliwość przywracania danych na poziomie poszczególnych plików oraz folderów w systemach Windows i Linux dla maszyn wirtualnych (możliwość wyodrębnienia dowolnego pliku/plików oraz katalogu/katalogów) z backupu obrazu maszyny wirtualnej.
9. Przywracanie plików z maszyny wirtualnej ma być niezależne i możliwe bez konieczności użycia platformy VMware (ESX lub vCenter).
10. Przywracanie maszyn wirtualnych ma być możliwe z przekierowaniem Hypervisora (zmiana miejsca docelowego dla odtwarzanego backupu) , jak również ma zapewnić możliwość wyboru data center, klastra lub hosta docelowego.
11. Agent backupu ma pozwalać na wykonanie backupu na poziomie bloków przy wsparciu technologi Raw Device Mapping (RDM) wraz z mechanizmem Changed Block Tracking (CBT).
12. Agent backupu ma integrować się z oprogramowaniem vCenter pozwalając na zarządzanie backupem na kilku hostach fizycznych.
13. Agent backupu ma wspierać rozwiązanie vApp, zapewniając backup grupy wspólnie pracujących maszyn.
14. System ma zapewniać zarządzanie zadaniami backupu i przywracania dla platformy wirtualnej z poziomu przeglądarki internetowej.
15. System ma wspierać wiele mechanizmów transportu, w szczególności system ma wspierać backup maszyn wirtualnych bez konieczności użycia sieci LAN (z wykorzystaniem sieci SAN), za pośrednictwem wirtualnej sieci LAN lub bezpośrednio na urządzenie podłączone za pośrednictwem interfejsu SCSI.
16. System ma mieć możliwość uaktywnienia mechanizmu deduplikacji danych dla backupu maszyn wirtualnych.
17. Funkcjonalność deduplikacji ma być możliwa zarówno na poziomie centralnego serwera backupu jak i po stronie backupowanej maszyny. Funkcjonalność ta ma być definiowana (także włączana lub wyłączana) na poziomie pojedynczego zadania backupu.
18. System ma mieć możliwość uaktywnienia kompresji danych dla backupu maszyn wirtualnych.
19. Administrator ma mieć możliwość wyboru pomiędzy przynajmniej dwoma algorytmami kompresji, przy czym produkt ma umożliwiać wybór minimum algorytmów LZRW1 oraz LZRW3-A.

IV. Agent do backupu środowiska wirtualnego Microsoft Hyper-V:

1. Agent backupu ma wspierać hot-backup (backup w czasie pracy) dla platformy wirtualizacyjnej Microsoft Hyper-V w wersjach Windows Server 2008 oraz Windows Server 2008 R2.
2. Backup ma być możliwy zarówno dla całych obrazów maszyn wirtualnych, jak i na poziomie poszczególnych wykorzystanych bloków.
3. Backup ma być realizowany jako backup pełny oraz backup inkrementacyjny z wykorzystaniem technologii śledzenia zmienionych bloków.
4. Funkcjonalność agenta backupu ma umożliwiać backup zarówno zatrzymanych jak również pracujących maszyn wirtualnych bez konieczności instalacji agenta na każdej z tych maszyn (backup na poziomie hypervisora).
5. Agent backupu ma umożliwiać backup tylko danych fizycznie zapisanych na wirtualnym dysku.
6. Agent backupu ma zapewniać możliwość przywracania wszystkich maszyn wirtualnych lub pojedynczych, zdefiniowanych przed administratora maszyn.
7. Przywracanie maszyn wirtualnych ma być niezależne. Proces przywracania nie ma wymagać od administratora wykorzystywania innych maszyn niż centralnego serwera backupu oraz docelowego hosta Hyper-V, na którym maszyny zostaną odtworzone.
8. Przywracanie maszyn wirtualnych ma być możliwe z przekierowaniem hypervisora (zmiana miejsca docelowego dla odtwarzanego backupu) ze wskazaniem hosta docelowego.
9. Agent backupu ma pozwalać na wykonanie backupu na poziomie bloków przy wsparciu mechanizmu Changed Block Tracking (CBT).
10. System ma zapewniać zarządzanie zadaniami backupu i przywracania dla platformy wirtualnej z poziomu przeglądarki internetowej.
11. System ma wspierać wiele mechanizmów transportu, w szczególności system ma wspierać backup maszyn wirtualnych bez konieczności użycia sieci LAN (z wykorzystaniem sieci SAN), za pośrednictwem wirtualnej sieci LAN lub bezpośrednio na urządzenie podłączone za pośrednictwem interfejsu SCSI.
12. System ma mieć możliwość uaktywnienia mechanizmu deduplikacji danych dla backupu maszyn wirtualnych.
13. Funkcjonalność deduplikacji ma być możliwa zarówno na poziomie centralnego serwera backupu jak i po stronie backupowanej maszyny. Funkcjonalność ta ma być definiowana (także włączana lub wyłączana) na poziomie pojedynczego zadania backupu.
14. System ma mieć możliwość uaktywnienia kompresji danych dla backupu maszyn wirtualnych.
15. System ma umożliwiać hot-backup aplikacji pracujących na maszynach wirtualnych z wykorzystaniem technologii VSS po stronie hypervisora bez konieczności instalacji agentów na każdej z maszyn wirtualnych.
16. Powyższa funkcjonalność ma umożliwiać hot-backup przynajmniej takich aplikacji jak: Mictosoft Exchange, Microsoft SQL Server, Microsoft Sharepoint oraz bazy danych Oracle.
17. System ma umożliwiać eksport pliku VHD z przeprowadzonego backupu na maszynę z systemem Windows 7 lub Windows 2008 celem zamontowania pliku obrazu i odzyskania poszczególnych plików z obrazu maszyny wirtualnej.
18. Administrator ma mieć możliwość wyboru pomiędzy przynajmniej dwoma algorytmami kompresji, przy czym produkt ma umożliwiać wybór minimum algorytmów LZRW1 oraz LZRW3-A.

V. Agent do backupu środowiska wirtualnego Xen oraz Citrix XenServer:

1. Agent backupu ma wspierać hot-backup (backup w czasie pracy) dla platform wirtualizacyjnych Xen oraz Citrix XenServer w wersjach 5.5 i wyższych.
2. Backup maszyn wirtualnych bez konieczności instalacji agenta na każdej z pracujących maszyn (backup na poziomie hypervisora).

3. Backup ma być realizowany jako backup pełny z uwzględnieniem wszystkich maszyn wirtualnych, zarówno pracujących jak również zatrzymanych.
4. Agent backupu ma zapewniać możliwość przywracania wszystkich maszyn wirtualnych lub pojedynczych, zdefiniowanych przed administratora maszyn.
5. Przywracanie maszyn wirtualnych ma być niezależne. Proces przywracania nie ma wymagać od administratora wykorzystywania innych maszyn niż centralnego serwera backupu oraz docelowego hosta Xen/XenServer na którym maszyny zostaną odtworzone.
6. Przywracanie maszyn wirtualnych ma być możliwe z przekierowaniem Hypervisora (zmiana miejsca docelowego dla odtwarzanego backupu) ze wskazaniem hosta docelowego.
7. System ma zapewniać zarządzanie zadaniami backupu i przywracania dla platformy wirtualnej z poziomu przeglądarki internetowej.
8. System ma wspierać wiele mechanizmów transportu, w szczególności system ma wspierać backup maszyn wirtualnych bez konieczności użycia sieci LAN (z wykorzystaniem sieci SAN), za pośrednictwem wirtualnej sieci LAN lub bezpośrednio na urządzenie podłączone za pośrednictwem interfejsu SCSI.
9. System ma mieć możliwość uaktywnienia mechanizmu deduplikacji danych dla backupu maszyn wirtualnych.
10. Funkcjonalność deduplikacji ma być możliwa zarówno na poziomie centralnego serwera backupu jak i po stronie backupowanej maszyny. Funkcjonalność ta ma być definiowana (także włączana lub wyłączana) na poziomie pojedynczego zadania backupu.
11. System ma mieć możliwość uaktywnienia kompresji danych dla backupu maszyn wirtualnych.
12. Administrator ma mieć możliwość wyboru pomiędzy przynajmniej dwoma algorytmami kompresji, przy czym produkt ma umożliwiać wybór minimum algorytmów LZRW1 oraz LZRW3-A.

VI. Mechanizm deduplikacji danych:

1. Program ma być wyposażony w technologię deduplikacji danych.
2. Deduplikacja ma działać w oparciu o technologię stałej długości bloku, przy czym długość ta zależna jest od wykrytego typu pliku. Niedopuszczalne jest stosowanie mechanizmów deduplikacji o zmiennej długości bloku lub o zawsze stałej długości, niezależnie od typu pliku.
3. Deduplikacja ma działać w oparciu o mechanizm identyfikacji typu pliku i na tej podstawie, dobierać optymalną wielkość bloku: inną dla dokumentu MS Word, inną dla prezentacji MS Powerpoint, inną dla arkusza MS Excel a jeszcze inną dla pliku maszyny wirtualnej VMDK. Program ma mieć wbudowaną bazę różnego typu plików wraz z odpowiadającymi im rozmiarami optymalnych długości bloku.
4. Administrator ma mieć możliwość określenia jakie typy plików będą deduplikowane jaką długością bloku. Funkcjonalność ta ma dawać przynajmniej możliwość zdefiniowania następujących długości bloków w bajtach dla poszczególnych typów plików: 1024, 2048, 4096, 8192, 16384, 32768, 65536.
5. Administrator ma mieć możliwość zdefiniowania (dla każdego z zadań backupu z osobna), czy deduplikacja będzie włączona czy nie oraz czy funkcja ta ma być realizowana na poziomie klienta (agenta) czy po stronie centralnego serwera backupu.
6. Mechanizm deduplikacji ma mieć możliwość operacji na dowolnych danych, w tym minimum pliki, bazy danych, maszyny wirtualne, poczta MS Exchange, MS Sharepoint jak i na każdych innych danych.
7. Mechanizm deduplikacji ma działać na dowolnym systemie operacyjnym klienta (agenta) w tym minimum na Windows, Linux, MacOS, FreeBSD, NetBSD, OpenBSD, Solaris.

VII. Mechanizm łańcuchowania D2D2T:

1. Oprogramowanie ma być wyposażone w funkcję łańcuchowania backupu Disk-To-Disk-To-Tape (D2D2T).
2. Funkcjonalność ta ma umożliwiać zdefiniowanie zadania backupu na dysk, które po zakończeniu automatycznie przeniesie dane na taśmę (za pośrednictwem napędu lub biblioteki taśmowej).

3. Administrator ma mieć możliwość zdefiniowania odstępu czasu wyrażonego w minutach, które opóźni moment przenoszenia danych na taśmę w stosunku do momentu zakończenia zadania backupu na dysk. Czas ten ma być definiowany per zadanie backupu.
4. Funkcjonalność łańcuchowania D2D2T ma być możliwa także dla backupów zaplanowanych z harmonogramu.
5. Przy definiowaniu zadania backupu z uaktywnionym łańcuchowaniem D2D2T administrator ma mieć możliwość określenia polityki wykorzystywania taśm (użycie istniejących taśm do końca lub wykorzystanie nowych taśm), określenia retencji dla backupu na taśmie oraz możliwość włączenia szczegółowego raportowania na e-mail o statusie zadania.
6. Administrator ma mieć możliwość zdefiniowania zautomatyzowanego mechanizmu D2D2T dla danych zapisanych na dysku, przy czym wyzwolenie zdarzenia łańcuchowania będzie związane minimum z: wielkością wykorzystywanego miejsca na wybranym zasobie dyskowym z dokładnością do 1MB, ilością pozostałego miejsca na zasobie dyskowym z dokładnością do 1MB.
7. Administrator ma mieć także możliwość zdefiniowania kolejności z jaką dane będą zapisywane na taśmie, minimum jako: od najstarszych do najnowszych lub od najnowszych do najstarszych.
8. Administrator ma mieć możliwość zdefiniowania czy po zakończeniu procesu łańcuchowania D2D2T dane na zasobie dyskowym mają być usunięte czy pozostawione.

CZĘŚĆ IV: Materiały eksploatacyjne do drukarek

Przedmiot dostawy musi być: fabrycznie nowy, nie regenerowany, wolny od wad technicznych i prawnych, dobrej jakości oraz dopuszczony do obrotu. Dopuszcza się tonery, tusze i bębny kompatybilne ze sprzętem, o parametrach takich samych lub lepszych niż wymienione poniżej.

Lp.	**Nazwa – model urządzenia**	**Minimalna wydajność stron A4 przy 5% pokryci/ pojemność**	**Ilość (szt.)**
1.	2.	3.	4.
1.	Toner do HP 2420	6 000	12
2.	Toner do HP 2100	5 000	6
3.	Toner do HP 1200	3 500	8
4.	Toner do HP 1100	2 500	6
5.	Toner do HP 1010	3 000	10
6.	Toner do HP 1300	4 000	8
7.	Toner do HP 1320	6 000	9
8.	Toner do HP 1150	2 500	10
9.	Toner do HP 3550 czarny	6 000	8
10.	Toner do HP 3550 żółty	4 000	8
11.	Toner do HP 3550 czerwony	4 000	8
12.	Toner do HP 3550 niebieski	4 000	8
13.	Toner do HP 3600n czarny	6 000	7
14.	Toner do HP 3600n żółty	4 000	7
15.	Toner do HP 3600n czerwony	4 000	7
16.	Toner do HP 3600n niebieski	4 000	7
17.	Toner do OKI C3200 czarny	1 500	5
18.	Toner do OKI C3200 żółty	1 500	5
19.	Toner do OKI C3200 cyan	1 500	5

20.	Toner do OKI C3200 magenta	1 500	5
21.	Toner OKI MC350 żółty	2 500	5
22.	Toner OKI MC350 czerwony	2 500	5
23.	Toner OKI MC350 niebieski	2 500	5
24.	Toner OKI MC350 czarny	2 500	5
25.	Toner do HP P1505 czarny	2 000	10
26.	Toner do HP P1566 czarny	2 000	10
27.	Tusz do HP 6122 czarny	42 ml	8
28.	Tusz do HP 6122/3820 kolor	38 ml	8
29.	Bęben światłoczuły czarny do OKI C3200	14 000	3
30.	Bęben światłoczuły żółty do OKI C3200	14 000	3
31.	Bęben światłoczuły cyan do OKI C3200	14 000	3
32.	Bęben światłoczuły magenta do OKI C3200	14 000	3
33.	Bęben światłoczuły OKI MC350 żółty	15 000	3
34.	Bęben światłoczuły OKI MC350 czerwony	15 000	3
35.	Bęben światłoczuły OKI MC350 niebieski	15 000	3
36.	Bęben światłoczuły OKI MC350 czarny	15 000	3

CZĘŚĆ V: Urządzenia drukujące i urządzenia wielofunkcyjne:

1. ***Kolorowe drukarki laserowe- 3 szt.***

Konfiguracja minimalna Zamawiającego		
1.	Rodzaj drukarki	laserowa
2.	Druk w kolorze	tak
3	Wyświetlacz	Tak, max. 3,5’
4.	Złącza	USB 2.0 zgodny wstecz z USB 1.1
5.	Rozdzielczość	w czerni: min. 600x600 dpi w kolorze: min. 600x600 dpi
6.	Szybkość druku	W kolorze min 12 str./min W mono 12 str./min
7.	Obciążenie normatywne	min. 20 000 str./miesiąc
8.	**Podajnik papieru**	150 arkuszy
9.	Taca odbioru papieru	125 arkuszy
10.	Obsługiwane formaty papieru	A4, A5, A6, B5
11.	Obsługiwane nośniki	Papier zwykły, papiery o gramaturze 60-163 g/m^2, koperta
12.	Druk dwustronny	ręczny
13.	Języki drukarkowe	PCL5, PCL6
14.	Obsługiwane systemy	MS Windows XP, Windows 7
15.	Tryby druku	Normalny, ekonomiczny (oszczędność tonera)
16.	Czas wydruku 1. strony	max 25 sekund
17.	Oprogramowanie	sterowniki, program instalacyjny, deinstalator dla systemów: MS Windows XP, Windows 7
18.	Kaseta z tonerem w komplecie	Drukarka ma być dostarczona z tonerami startowymi (nowe i nieużywane).
19.	Bezpłatne Wsparcie Techniczne	Dostępne na witrynie producenta sprzętu sterowniki i

		informacje techniczne dotyczące oferowanego produktu .
20.	Gwarancja	Min. 1 rok
21.	Kabel	Min. 3 m USB 2.0 do połączenia z komputerem

2. ***Drukarki monochromatyczne laserowe- 3 szt.***

Konfiguracja minimalna Zamawiającego		
1.	Rodzaj drukarki	laserowa
2.	Pamięć	min.8 MB
3.	Złącza	USB 2.0 zgodny wstecz z USB 1.1
4.	Rozdzielczość	min. 600x600 dpi
5.	Szybkość druku:	min. 16 str./min
6.	Obciążenie normatywne	min. 4 000 str./miesiąc
7.	Taca odbioru papieru	150 arkuszy A4
8.	Obsługiwane formaty papieru	A4, A5, Letter
9.	Obsługiwane nośniki	Papier zwykły, papiery o gramaturze 60-163 g/m^2, koperta
10.	Druk dwustronny	ręczny
11.	Języki drukarkowe	PCL5, PCL6
12.	Obsługiwane systemy	MS Windows XP, Windows 7
13.	Tryby druku	Normalny, ekonomiczny (oszczędność tonera)
14.	Czas wydruku 1. strony	max 12 sekund
15.	Oprogramowanie	sterowniki, program instalacyjny, deinstalator dla systemów: MS Windows XP, Windows 7
16.	Kaseta z tonerem w komplecie	Drukarka ma być dostarczona z tonerami startowymi (nowe i nieużywane).
17.	Bezpłatne Wsparcie Techniczne	Dostępne na witrynie producenta sprzętu sterowniki i informacje techniczne dotyczące oferowanego produktu .
23.	Gwarancja	1 rok
24.	Kabel	Min. 3 m USB 2.0 do połączenia z komputerem

3. ***Urządzenie wielofunkcyjne atramentowe- 2 szt.***

Konfiguracja minimalna Zamawiającego		
1.	Obsługiwane funkcje	Drukarka, Skaner, Kopiarka
2.	Funkcje obsługiwane bez włączonego komputera	Kserokopiarka
3.	Technologia druku	atramentowa
4.	Druk dwustronny	ręczny
5.	Interfejs podłączenia	USB 2.0, kompatybilne wstecz z USB 1.1
6.	Kaseta z tuszami w komplecie	Kaseta zawierająca komplet tuszy startowych
7.	Szybkość druku w czerni	8 str./min
8.	Szybkość druku w kolorze	5str./min
9.	Rozdzielczość druku w czerni	600 x 600 dpi
10.	Rozdzielczość druku w kolorze	1 200 x 1 200 dpi
11.	Czas wydruku pierwszej strony	Maksymalnie 18 sek.
12.	Typ skanera	Płaski
13.	Optyczna rozdzielczość skanowania	1 200 x 1 200 dpi
14.	Głębia koloru skanowania	24bity
15.	Obszar skanowania	A4
16.	Szybkość kopiowania	4 strony na minutę
17.	formaty papieru	A4, A5, koperta
18.	Obsługiwane nośniki	Papier zwykły, papier fotograficzny, koperty

19.	Obsługiwane języki drukarek	PCL3
20.	Pojemność podajników papieru:	50 arkuszy
21.	Pojemność tacy odbiorczej	25 arkuszy
22.	Obsługiwane systemy	MS Windows XP/Windows 7
23.	Obsługiwane formaty dokumentów	PDF
24.	Certyfikaty i oświadczenia	Deklaracja producenta spełnienia przez sprzęt wymaganych norm CE - załączona do oferty. Certyfikat Energy Star w wersji co najmniej 4.0 dla oferowanego modelu - kopia załączona do oferty.
25.	Bezpłatne Wsparcie Techniczne	Dostępne na witrynie producenta sprzętu sterowniki, uaktualnienia, parametry materiałów eksploatacyjnych, oraz informacje techniczne dotyczące oferowanego typu urządzenia.
26.	Gwarancja:	1 rok
27.	Kabel	Min. 3 m USB 2.0 do połączenia z komputerem