Załącznik nr 4 do SIWZ

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2007-2013 oraz z budżetu państwa.

Spis treści

1. Serwer blade

1.1. Obudowa blade

Producent …….....

Model …….....…...

spełniający poniższe wymagania minimalne:

1 sztuka

L.P.	Nazwa elementu	Wymagania techniczne
1.	Obudowa	Obudowa nie wyższa niż 10U, dostosowana do szafy *rack* 19”, komplet kabli i przewodów połączeniowych niezbędnych do podłączenia zaoferowanego rozwiązania. Należy zapewnić możliwość instalacji minimum 16 modułów serwerowych w dostępnych wnękach obudowy.
2.	Sposób agregacji/wyprowadzeń sygnałów LAN	Obudowa musi posiadać min. 2 moduły komunikacyjne 10Gb Ethernet pozwalające na logiczną separację portów oraz ich łączenie za pomocą logicznych mechanizmów typu *switch*. Moduły muszą wspierać mechanizm logicznej separacji łącz wychodzących z serwerów z zachowaniem redundancji połączeń. Każdy moduł musi posiadać 16 portów 10Gb (wewnętrznych) – do podłączenia modułów serwerowych blade. Każdy moduł musi posiadać minimum 8 wyjściowych portów zewnętrznych. Wszystkie porty muszą być wyposażone w odpowiednie moduły SFP/SFP+ (min. 6 portów RJ45 1Gb, 2 porty LC SR 10Gb).
3.	Sposób agregacji/wyprowadzeń sygnałów FC	Dwa moduły FibreChannel 8Gb/s, każdy posiadający 24 porty aktywne: min. 16 portów wewnętrznych, 8 portów zewnętrznych obsadzonych wkładkami SFP/SFP+ 8Gb FC wraz z wszystkimi licencjami dostępnymi dla oferowanego modelu.
4.	Wirtualizacja połączeń	W obrębie pojedynczej obudowy dostarczone moduły komunikacyjne LAN i SAN muszą umożliwiać wirtualizację połączeń i interfejsów LAN i SAN w serwerach blade poprzez możliwość przydzielania adresów WWN i MAC dla serwerów niezależnie od fabrycznych adresów na fizycznych kartach. Musi istnieć także możliwość przenoszenia przydzielonych adresów pomiędzy wnękami w obudowie. Dodatkowo dla sieci LAN musi istnieć możliwość stworzenia niezależnych połączeń tak aby między wydzielonymi sieciami nie było komunikacji. Tak wydzielone połączenie wirtualne musi być widziane z

		poziomu hypervisora zainstalowanego na module serwerowym blade jako fizyczna karta sieciowa. Musi istnieć możliwość określenia pasma przepustowości dla tak stworzonego pojedynczego portu LAN na serwerze od 100Mb/s do 10Gb/s.
5.	Zasilanie	- Redundantne zasilacze wymienne w trakcie pracy, pozwalające na zasilenie w pełni obsadzonej obudowy blade (min. 16 modułów serwerowych) - Redundancja typu N+N - Wymaga się, aby utrata co najmniej połowy zasilaczy nie powodowała zatrzymania lub zmniejszenia wydajności serwerów zainstalowanych w obudowie - Obudowa powinna umożliwiać optymalizowanie obciążenia zainstalowanych zasilaczy celem osiągnięcia maksymalnej sprawności pracy zasilaczy i minimalizacji zużycia energii. - 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).
6.	Zarządzanie	Wymaga się, aby dostarczone rozwiązanie było wyposażone w dwie, redundantne karty zarządzające (tzw. Management blade) umożliwiające/ wyposażone w: - pełna administracja chassis za pośrednictwem interfejsu Web - dedykowany port serwisowy LAN RJ-45 dla każdej karty zarządzającej - funkcję KVM realizowaną dla każdego z modułów serwerowych - system zarządzania musi umożliwiać wymianę modułu serwerowego przy pomocy logicznego profilu obejmującego konfigurację modułu serwerowego w zakresie sieci LAN i SAN. W zakres logicznego profilu serwerowego muszą wchodzić minimum następujące parametry: adres MAC, adres WWNN/WWPN, sekwencja bootowania systemu, sposób konfiguracji oraz cechy adapterów NIC i HBA - system zarządzania musi posiadać funkcje centralnego zarządzanie adresami MAC oraz adresami WWNN/WWPN serwerów - dostarczona infrastruktura serwerowa powinna pracować bez przerw czy obniżenia wydajności serwerów nawet w przypadku uszkodzenia obydwóch modułów zarządzających - zarządzanie poszczególnymi modułami serwerowymi (przejęcie ich konsoli w trybie graficznym i tekstowym – także w sesji BIOS, podłączenie wirtualnych napędów) - zarządzanie jednocześnie wszystkimi modułami serwerowymi - zdalna identyfikacja modułu serwerowego 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
7.	Wentylacja	System musi zapewniać sprawną wentylację w pełni obsadzonej obudowy blade (min. 16 modułów serwerowych) nie dopuszczając do przegrzania zamontowanych modułów serwerowych. Wentylatory muszą być redundantne typu Hot-Plug.
8.	Gwarancja	Co najmniej 36 miesięcy gwarancji producenta. W ramach gwarancji Zamawiający powinien mieć dostęp za pośrednictwem witryny www producenta sprzętu do aktualizacji oprogramowania wewnętrznego serwera (firmware) wszystkich komponentów od momentu zakupu oraz po okresie gwarancji – wsparcia.
9.	Dokumentacja	Komplet dokumentacji: instrukcja obsługi, użytkowania interfejsów zarządzających, procedur obsługi błędów w języku polskim lub angielskim.

1.2. Moduł serwerowy

Producent …….....

Model …….....…...

spełniający poniższe wymagania minimalne:

8 sztuk

L.P.	Nazwa elementu	Wymagania techniczne
1.	Obudowa	Typu blade, umożliwiająca zainstalowanie min. 16 sztuk zaoferowanych modułów serwerowych w dostarczanej wraz z modułami serwerowymi obudowie Blade.
2.	Procesory	Co najmniej 2 zainstalowane procesory x86_64 posiadające min. 8 rdzeni obliczeniowych każdy, umożliwiający osiągnięcie wyniku min. 490 punktów w teście SPECint_rate_base2006 dla serwera referencyjnego z zainstalowanymi dwoma takimi procesorami. Nie wymaga się by oferowany serwer (np. producent, model) był identyczny z serwerem referencyjnym opisanym na stronie www.spec.org. Wystarczy, że posiada ten sam zestaw procesorów.
3.	Pamięć RAM	Min.128GB pamięci RAM ECC z możliwością rozbudowy do co najmniej 512GB bez wymiany już obsadzonych banków. Z

		symetrycznym rozłożeniem na zainstalowane procesory.
4.	Przestrzeń dyskowa	Redundantna przestrzeń flash (zamontowana wewnątrz obudowy modułu serwerowego) na potrzeby ładowania hypervisora (np. karty SD, CF, usb-flash)
5.	Interfejsy sieciowe (LAN)	Redundantna ilość interfejsów sieci LAN 10Gbps(minimum 2). Interfejsy muszą wspierać mechanizmy wirtualizacji połączeń sieciowych (virtual NIC). Dla jednego interfejsu LAN musi być możliwość podziału na min. 4 wirtualne karty sieciowe (posiadające własne adresy MAC oraz będące widoczne z poziomu systemu operacyjnego jako fizyczne karty sieciowe). Podział musi być niezależny od zainstalowanego na serwerze systemu operacyjnego/platformy wirtualizacyjnej.
6.	Interfejsy FC do podłączenia zewnętrznych zasobów dyskowych	Co najmniej dwa interfejsy FC 8Gbps, Zamawiający dopuszcza możliwość wirtualizacji tych połączeń w podobny sposób jak połączenia sieci LAN.

1.3. Szafa rack

Producent …….....

Model …….....…...

spełniający poniższe wymagania minimalne:

1 sztuka

L.P.	Wymagania techniczne
1.	42U pojemności użytecznej do instalacji urządzeń w pozycji poziomej
2.	4U pojemności użytecznej do instalacji urządzeń w pozycji pionowej (np. kvm,switche,itp.)
3.	Całkowita głębokość min. 1000mm.
4.	Całkowita szerokość min. 800mm.
5.	Klasa ochrony IP20.
6.	Wyposażona w przednie drzwi perforowane, zamykane na zamek z kluczem, jednoskrzydłowe, możliwość montażu lewa/prawa strona.
7.	Wyposażona w tylne drzwi perforowane, dwuskrzydłowe dla ograniczenia przestrzeni serwisowej, zamykane na zamek z kluczem wspólny z zamkiem przednim.
8.	Wyposażona w zdejmowane panele boczne zabezpieczone w taki sam sposób jak drzwi.

9.	Wentylacja aktywna (panel z 4 wentylatorami) wyposażona w termostat.
10.	Co najmniej 2 listwy zasilające po min. 8 gniazd każda. Gniazda powinny być zgodne z typem okablowania dostarczonym wraz z elementami Systemu instalowanymi w PCPD.
11.	Możliwość wyposażenia w fabryczne zabezpieczenie teleskopowe przeciwko wywróceniu szafy do przodu (tzw. tiltprotection).
12.	Udźwig gwarantowany szafy co najmniej 840 kg.
13.	Przystosowana do poprawnej instalacji dostarczonego rozwiązania.
14.	Fabryczna możliwość trwałego łączenia wielu szaf jednakowego typu.

1.4. System wirtualizacji

Producent …….....

Nazwa, wersja …….....

Ilość …….....

spełniający poniższe wymagania minimalne:

L.P.	Funkcje
1.	Licencje powinny umożliwiać uruchomianie wirtualizacji (pełne wykorzystanie procesorów i pamięci operacyjnej) na wszystkich dostarczonych modułach serwerowych (min. 8szt), każdy z zainstalowaną pamięcią RAM min. 128GB oraz 1 konsoli do zarządzania całym środowiskiem. Wszystkie licencje powinny być dostarczone wraz z 3-letnim wsparciem, świadczonym przez producenta oprogramowania wirtualnego na pierwszej, drugiej i trzeciej linii wsparcia. Wsparcie powinno umożliwiać zgłaszanie problemów 5 dni w tygodniu przez 12 godzin
2.	Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez konieczności instalacji systemu operacyjnego
3.	Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej modułu serwerowego.
4.	Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym module serwerowym i musi się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. Wymagana jest możliwość przydzielenia maszynie większej ilości wirtualnej pamięci operacyjnej, niż jest zainstalowana w module serwerowym oraz większej ilości przestrzeni dyskowej niż jest fizycznie dostępna.
5.	Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows NT, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, SLES 11, SLES 10, SLES9, SLES8, Ubuntu 7.04, RHEL 5, RHEL 4,

	RHEL3, RHEL 2.1, Solaris wersja 10 dla platformy x86, NetWare 6.5, NetWare 6.0, NetWare 6.1, Debian, CentOS, FreeBSD, Asianux, Ubuntu 7.04, SCO OpenServer, SCO Unixware, Mac OS X.
6.	Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
7.	Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
8.	Rozwiązanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania trybu XP mode w Windows 7, a także instalacji wszystkich funkcjonalności w tym Hyper-V pakietu Windows Server 2012 na maszynie wirtualnej.
9.	Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania środowiskiem serwerów wirtualnych. Konsola graficzna musi być dostępna poprzez dedykowanego klienta i za pomocą przeglądarek, minimum IE i Firefox.
10.	Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.
11.	Rozwiązanie musi umożliwiać pozyskiwanie danych wydajnościowych o pracujących maszynach wirtualnych przez rozwiązania firm trzecich bezpośrednio z silnika bazy danych poprzez ODBC
12.	Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich modułów serwerowych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root.
13.	Rozwiązanie musi umożliwiać składowanie logów ze wszystkich modułów serwerowych i konsoli zarządzającej na serwerze Syslog. Serwer Syslog w dowolnej implementacji musi stanowić integralną część rozwiązania.
14.	Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej i zdefiniowania alertów informujących o przekroczeniu wartości progowych.
15.	Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.
16.	Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej tak, aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.
17.	Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie.
18.	Kopie zapasowe powinny być składowane z wykorzystaniem technik de-duplikacji danych.
19.	Musi istnieć możliwość odtworzenia pojedynczych plików z kopii zapasowej maszyny wirtualnej przez osoby do tego upoważnione bez konieczności nadawania takim osobom bezpośredniego dostępu do głównej konsoli zarządzającej całym środowiskiem.
20.	Mechanizm zapewniający kopie zapasowe musi być wyposażony w system cyklicznej kontroli

	integralności danych. Ponadto musi istnieć możliwość przywrócenia stanu repozytorium kopii zapasowych do punktu w czasie, kiedy wszystkie dane były integralne w przypadku jego awarii.
21.	Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
22.	Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi.
23.	Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
24.	Platforma wirtualizacyjna musi umożliwiać zastosowanie w modułach serwerowych procesorów o dowolnej ilości rdzeni.
25.	Rozwiązanie musi umożliwiać tworzenie jednorodnych wolumenów logicznych o wielkości 64TB.
26.	Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
27.	Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
28.	Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy modułami serwerowymi oraz pamięciami masowymi nie zależnie od dostępności współdzielonej przestrzeni dyskowej.
29.	Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy modułami serwerowymi.
30.	Typowy czas niedostępności usług w przypadku awarii lub niedostępności modułu serwerowego nie powinien przekraczać kilkunastu minut.
31.	Dla wybranych maszyn wirtualnych musi istnieć rozwiązanie zapewniające nieprzerwaną ich pracę na wypadek awarii lub niedostępności modułu serwerowego.
32.	Rozwiązanie musi zakładać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej lub partycjonowania sieci.
33.	Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności modułu serwerowego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu, po jakim taka decyzja jest wykonywana.
34.	Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury.
35.	Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty

	sprzętu, lub oprogramowania.
36.	Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa, jak i podnoszenie jej wersji.
37.	Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych modułów serwerowych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania.
38.	Rozwiązanie musi gromadzić i umożliwiać zunifikowaną, graficzną prezentację informacji o wszystkich aspektach infrastruktury serwerów wirtualnych z uwzględnieniem danych szczegółowych takich jak poziom obciążenia sieci czy ilość IOPS w komunikacji z pamięcią masową.
39.	Zgromadzone dane muszą zapewniać ocenę kondycji, wydajności i pojemności dowolnego elementu infrastruktury, wliczając centrum danych, klastry, moduły serwerowe, podsystemy dyskowe i grupy maszyn wirtualnych. Ocena ta powinna być wartością jednowymiarową wyliczoną na podstawie agregacji zgromadzonych danych szczegółowych.
40.	Dostęp do warstwy prezentacji wyników analiz wydajnościowo pojemnościowych musi być możliwy przez dedykowanego klienta oraz przez przeglądarkę internetową.
41.	Uprawnienia do warstwy prezentacji wyników muszą dopuszczać rozłączność z uprawnieniami do infrastruktury.
42.	Rozwiązanie musi precyzyjnie określać na podstawie aktualnej i historycznej dynamiki rozwoju infrastruktury pozostałą pojemność i czas pozostały do przewidywanego wysycenia zasobów.
43.	Progi alertowe muszą być generowane dynamicznie na podstawie zebranych danych z infrastruktury i trybie ciągłym korygowane na podstawie aktualnego obciążenia i pozostałej pojemności infrastruktury.
44.	Musi istnieć możliwość ręcznego przełączenia na rozwiązanie zapasowe, a także powrotu pracy na rozwiązanie podstawowe.
45.	Rozwiązanie musi zapewniać integrację z warstwą aplikacyjną tak, aby na wypadek awarii komponentu programowego nastąpiło automatyczne przełączenie na rozwiązanie zapasowe, niezależnie od awarii sprzętu.
46.	Mechanizmy wysokiej dostępności muszą być zapewnione niezależnie od wyboru platformy ich implementacji, tzn. muszą działać tak samo dla instalacji komponentów zarządzających na modułach serwerowych, wirtualnych i w środowisku mieszanym.
47.	Rozwiązanie musi posiadać architekturę active-standby tak, aby w świetle postanowień licencyjnych firm trzecich redundancja była rozumiana jako rozwiązanie zapasowe, nie aktywne przy normalnej pracy rozwiązania podstawowego.
48.	Rozwiązanie musi być rozłączne (nadmiarowe) w stosunku do istniejącego mechanizmu zapewniania wysokiej dostępności wbudowanego w warstwę wirtualizacji.
49.	Rozwiązanie musi posiadać mechanizmy zapewniania wysokiej dostępności komponentów

	zarządzających w taki sposób, aby umożliwić nieprzerwany dostęp do konsoli zarządzającej w przypadku awarii pojedynczego modułu serwerowego.
50.	Rozwiązanie musi umożliwiać tworzenie wirtualnych przełączników dystrybuowanych w obrębie projektowanego środowiska wirtualnego

2. Macierz dyskowa podstawowa w PCPD

Producent …….....

Model …….....…...

spełniający poniższe wymagania minimalne:

1 sztuka

L.P.	Nazwa elementu	Wymagania techniczne
1.	Kontroler	Dwa symetryczne kontrolery pracujące w trybie Active/Active
2.	Pamięć podręczna	Min. 32GB pamięci podręcznej na kontroler, Zamawiający nie dopuszcza rozwiązania używającego dodatkowej pamięci typu flash jako pamięci podręcznej.
3.	Przestrzeń dyskowa	Minimalna ilość dysków oraz ich minimalne parametry: • 96 szt. dysków 2,5” SAS, 600GB, • 40 szt. dysków 3,5” NL-SAS, 3TB, URE >= 10^{15}
4.	Porty komunikacyjne	Co najmniej 4 porty Fibre Channel 8 Gbps. Możliwa rozbudowa o kolejne 4 porty FC lub 4 porty iSCSI
5.	Kable połączeniowe	Wykonawca dostarczy wymaganą dla rozwiązania ilość i rodzaj przewodów połączeniowych z zachowaniem redundancji
6.	Przełącznik FC	2 szt. przełączników FC o wysokości maksymalnie 1U z możliwością montażu w szafie Rack 19” o poniższych właściwościach: - minimum 10 slotów na moduły FC. Wymagane jest dostarczenie licencji (na pełną funkcjonalność) dla wszystkich portów FC przełącznika - moduły SFP: 8 x SFP Short Wave 8 Gbit oraz 2 x SFP Long Wave 8Gbit dla odległości min. 5km, W przypadku gdy oferowane rozwiązanie wymaga większej ilości Wykonawca powinien je dostarczyć - typy portów FC: przełącznik FC musi być wykonany w technologii FC 8 Gb/s i posiadać możliwość pracy portów FC z prędkościami 8, 4, 2 Gb/s z funkcją auto-negocjacji prędkości

		- obsługa modułów SFP: przełącznik FC musi mieć możliwość instalacji jednomodowych modułów SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 5km - przepustowość: zsumowana przepustowość przełącznika FC musi wynosić minimum 640 Gbit/sec end-to-end full duplex - protokoły Fibre Channel: FL_Port, F_Port, E_Port, EX_Port, M_Port (Mirror Port), and self-discovery based on switch type (U_Port) - typy komunikacji: unicast, multicast (255 group), and broadcast - obsługa standardów: Telnet, SNMP - klasy obsługi: Class 2, Class 3, Class F - zarządzanie przełącznikiem: przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym. Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany 10/100 port Ethernet oraz serial port.

Wymagania funkcjonalne	
L.P.	**Funkcje**
1.	Macierz musi obsługiwać następujące systemy operacyjne: IBM AIX, HP-UX, Sun Solaris, Linux, Microsoft Windows Server 2003, 2008, 2012. Jeżeli funkcjonalność taka wymaga dodatkowych licencji, to należy je uwzględnić w ofercie.
2.	Macierz musi wspierać następujące typy dysków: SAS, NL-SAS i SSD
3.	Macierz musi gwarantować możliwość rozbudowy on-line do co najmniej 480 dysków, bez konieczności wymiany kontrolerów, wykonywania migracji oraz odzyskiwania danych z kopii zapasowych. Jeżeli funkcjonalność taka wymaga dodatkowych licencji, to należy je uwzględnić w ofercie.
4.	Każdy z kontrolerów musi być wyposażony w co najmniej 32GB pamięci cache z możliwością rozbudowy do 64GB
5.	Macierz musi mieć możliwość migracji wolumenów logicznych (LUN) pomiędzy różnymi grupami dyskowymi RAID w obrębie macierzy. Migracja musi być wykonywana w trybie on-line. Jeżeli funkcjonalność taka wymaga dodatkowych licencji, to należy je uwzględnić w ofercie.
6.	Macierz musi umożliwiać rozbudowę istniejących grup dyskowych RAID o dodatkowe

	dyski w trybie on-line (bez przerywania pracy aplikacji). Jeżeli funkcjonalność taka wymaga dodatkowych licencji, to należy je uwzględnić w ofercie.
7.	Macierz musi umożliwiać zwiększanie pojemności wolumenów logicznych LUN w trybie on-line. Jeżeli funkcjonalność taka wymaga dodatkowych licencji, to należy je uwzględnić w ofercie.
8.	Macierz musi posiadać min. 4 porty zewnętrzne Fibre Channel o paśmie przepustowości 8Gb/s dla każdego z portów.
9.	Macierz musi posiadać możliwość podłączania do niej wielu serwerów z różnymi systemami operacyjnymi w taki sposób, aby każdy z podłączonych serwerów miał dostęp tylko do swoich wolumenów logicznych (LUN masking). Jeżeli funkcjonalność taka wymaga dodatkowych licencji, to należy je uwzględnić w ofercie.
10.	Macierz musi zapewniać możliwość uaktualniania mikrokodu bez przerywania pracy systemu.
11.	Macierz musi zapewniać możliwość wymiany dysków podczas pracy systemu (hot-swap)
12.	Macierz musi zapewniać możliwość utworzenia co najmniej 4096 wolumenów logicznych LUN
13.	Macierz musi zapewniać obsługę technologii RAID: 1, 10, 5 oraz 6 (podwójna parzystość). Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID-5 i RAID-6 powinno być realizowane w sposób sprzętowy przez dedykowany układ w macierzy.
14.	Wszystkie krytyczne komponenty macierzy: kontrolery, zasilacze, wentylatory muszą pracować w trybie nadmiarowym, tak aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego SYSTEMU. Komponenty te muszą być wymienialne w trakcie pracy macierzy.
15.	Macierz musi oferować zarządzanie poprzez sieć LAN.
16.	Macierz musi umożliwiać instalację w szafie *rack* 19”.
17.	Macierz powinna być dostarczona z oprogramowaniem pozwalającym na zarządzanie pełną (maksymalną) pojemnością macierzy. Jeżeli funkcjonalność taka wymaga dodatkowych licencji, to należy je uwzględnić w ofercie.
18.	Macierz musi obsługiwać poprzez wewnętrzne mechanizmy firmware’u kopiowanie pełne (klonowanie) oraz wykonywanie min. 512 migawek (snapshotów). Jeżeli funkcjonalność taka wymaga dodatkowych licencji, to należy je uwzględnić w ofercie.
19.	Macierz musi obsługiwać poprzez wewnętrzne mechanizmy firmware’u replikację zdalną synchroniczną i asynchroniczną.
20.	Macierz musi obsługiwać QoS (Quality of Services) czyli nadawanie priorytetów obsługi

	transmisji I/O dla skonfigurowanych hostów, LUN-ów, portów do hostów. Jeżeli funkcjonalność ta wymaga odrębnej licencji należy dostarczyć ja wraz z macierzą w wariancie dla maksymalnej pojemności dyskowej danej macierzy.
21.	Macierz musi obsługiwać mechanizmy ograniczania wielkości pamięci podręcznej cache do obsługi wybranych woluminów LUN – tzw. cache partitioning. Jeżeli funkcjonalność ta wymaga odrębnej licencji należy dostarczyć ja wraz z macierzą w wariancie dla maksymalnej pojemności dyskowej danej macierzy oraz dla maksymalnej ilości obsługiwanych woluminów.
22.	Macierz musi posiadać funkcjonalność tieringu. Jeżeli funkcjonalność ta wymaga odrębnej licencji należy dostarczyć ja wraz z macierzą.
23.	Oprogramowanie do zarządzania macierzą musi być zintegrowane z systemem operacyjnym systemu pamięci masowej bez konieczności dedykowania oddzielnego serwera do obsługi tego oprogramowania.
24.	Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.
25.	Macierz musi posiadać wbudowaną funkcjonalność typu thinprovisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości.

Załącznik nr 4 do SIWZ

3. Macierz dyskowa zapasowa w ZCPD

Producent …….....

Model …….....…...

spełniający poniższe wymagania minimalne:

1 sztuka

L.P.	Nazwa elementu	Wymagania techniczne
1.	Kontroler	Dwa symetryczne kontrolery pracujące w trybie Active/Active
2.	Pamięć podręczna	Min. 32GB pamięci podręcznej na kontroler, Zamawiający nie dopuszcza rozwiązania używającego dodatkowej pamięci typu flash jako pamięci podręcznej.
3.	Przestrzeń dyskowa	Minimalna ilość dysków oraz ich minimalne parametry: • 72 szt. dysków 3,5” NL-SAS, 3TB, URE >= 10^{15}
4.	Porty komunikacyjne	Co najmniej 4 porty Fibre Channel 8 Gbps. Możliwa rozbudowa o kolejne 4 porty FC lub 4 porty iSCSI
5.	Kable połączeniowe	Wykonawca dostarczy wymaganą dla rozwiązania ilość i rodzaj przewodów połączeniowych z zachowaniem redundancji.
6.	Przełącznik FC	2 szt. przełączników FC o wysokości maksymalnie 1U z możliwością montażu w szafie Rack 19” o poniższych właściwościach: - minimum 8 slotów na moduły FC. Wymagane jest dostarczenie licencji (na pełną funkcjonalność) dla wszystkich portów FC przełącznika - moduły SFP: 6 x SFP Short Wave 8 Gbit oraz 2 x SFP Long Wave 8Gbit dla odległości min. 5km, W przypadku gdy oferowane rozwiązanie wymaga większej ilości Wykonawca powinien je dostarczyć - typy portów FC: przełącznik FC musi być wykonany w technologii FC 8 Gb/s i posiadać możliwość pracy portów FC z prędkościami 8, 4, 2 Gb/s z funkcją auto-negocjacji prędkości - obsługa modułów SFP: przełącznik FC musi mieć możliwość instalacji jednomodowych modułów SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 5km - przepustowość: zsumowana przepustowość przełącznika FC

		musi wynosić minimum 640 Gbit/sec end-to-end full duplex - protokoły Fibre Channel: FL_Port, F_Port, E_Port, EX_Port, M_Port (Mirror Port), and self-discovery based on switch type (U_Port) - typy komunikacji: unicast, multicast (255 group), and broadcast - obsługa standardów: Telnet, SNMP - klasy obsługi: Class 2, Class 3, Class F - zarządzanie przełącznikiem: przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym. Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany 10/100 port Ethernet oraz serial port.
7.	Szafa rack	1 szt. szafy serwerowej rack 19” o poniższych właściwościach: - 42U pojemności użytecznej do instalacji urządzeń w pozycji poziomej, - 4U pojemności użytecznej do instalacji urządzeń w pozycji pionowej (np. kvm,switche,itp.), - Całkowita głębokość min. 1000mm, - Całkowita szerokość min. 800mm, - Klasa ochrony IP20, - Wyposażona w przednie drzwi perforowane, zamykane na zamek z kluczem, jednoskrzydłowe, możliwość montażu lewa/prawa strona, - Wyposażona w tylne drzwi perforowane, dwuskrzydłowe dla ograniczenia przestrzeni serwisowej, zamykane na zamek z kluczem wspólny z zamkiem przednim, - Wyposażona w zdejmowane panele boczne zabezpieczone w taki sam sposób jak drzwi, - Wentylacja aktywna (panel z 4 wentylatorami) wyposażona w termostat, - Co najmniej 2 listwy zasilające po min. 8 gniazd każda, - Gniazda powinny być zgodne z typem okablowania dostarczonym wraz z elementami Systemu instalowanymi w ZPCD, - Możliwość wyposażenia w fabryczne zabezpieczenie teleskopowe przeciwko wywróceniu szafy do przodu (tzw. tiltprotection), - Udźwig gwarantowany szafy co najmniej 840 kg, - Przystosowana do poprawnej instalacji dostarczonego rozwiązania, - Fabryczna możliwość trwałego łączenia wielu szaf jednakowego typu.

Załącznik nr 4 do SIWZ

Wymagania funkcjonalne	
L.P.	**Funkcje**
1.	Macierz musi obsługiwać następujące systemy operacyjne: IBM AIX, HP-UX, Sun Solaris, Linux, Microsoft Windows Server 2003, 2008, 2012. Jeżeli funkcjonalność taka wymaga dodatkowych licencji, to należy je uwzględnić w ofercie.
2.	Macierz musi wspierać następujące typy dysków: SAS, NL-SAS i SSD
3.	Macierz musi gwarantować możliwość rozbudowy on-line do co najmniej 480 dysków, bez konieczności wymiany kontrolerów, wykonywania migracji oraz odzyskiwania danych z kopii zapasowych. Jeżeli funkcjonalność taka wymaga dodatkowych licencji, to należy je uwzględnić w ofercie.
4.	Każdy z kontrolerów musi być wyposażony w co najmniej 32GB pamięci cache z możliwością rozbudowy do 64GB
5.	Macierz musi mieć możliwość migracji wolumenów logicznych (LUN) pomiędzy różnymi grupami dyskowymi RAID w obrębie macierzy. Migracja musi być wykonywana w trybie on-line. Jeżeli funkcjonalność taka wymaga dodatkowych licencji, to należy je uwzględnić w ofercie.
6.	Macierz musi umożliwiać rozbudowę istniejących grup dyskowych RAID o dodatkowe dyski w trybie on-line (bez przerywania pracy aplikacji). Jeżeli funkcjonalność taka wymaga dodatkowych licencji, to należy je uwzględnić w ofercie.
7.	Macierz musi umożliwiać zwiększanie pojemności wolumenów logicznych LUN w trybie on-line. Jeżeli funkcjonalność taka wymaga dodatkowych licencji, to należy je uwzględnić w ofercie.
8.	Macierz musi posiadać min. 4 porty zewnętrzne Fibre Channel o paśmie przepustowości 8Gb/s dla każdego z portów.
9.	Macierz musi posiadać możliwość podłączania do niej wielu serwerów z różnymi systemami operacyjnymi w taki sposób, aby każdy z podłączonych serwerów miał dostęp tylko do swoich wolumenów logicznych (LUN masking). Jeżeli funkcjonalność taka wymaga dodatkowych licencji, to należy je uwzględnić w ofercie.
10.	Macierz musi zapewniać możliwość uaktualniania mikrokodu bez przerywania pracy systemu.
11.	Macierz musi zapewniać możliwość wymiany dysków podczas pracy systemu (hot-swap)
12.	Macierz musi zapewniać możliwość utworzenia co najmniej 4096 wolumenów logicznych LUN
13.	Macierz musi zapewniać obsługę technologii RAID: 1, 10, 5 oraz 6 (podwójna parzystość).

	Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID-5 i RAID-6 powinno być realizowane w sposób sprzętowy przez dedykowany układ w macierzy.
14.	Wszystkie krytyczne komponenty macierzy: kontrolery, zasilacze, wentylatory muszą pracować w trybie nadmiarowym, tak aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego SYSTEMU. Komponenty te muszą być wymienialne w trakcie pracy macierzy.
15.	Macierz musi oferować zarządzanie poprzez sieć LAN.
16.	Macierz musi umożliwiać instalację w szafie *rack* 19”.
17.	Macierz powinna być dostarczona z oprogramowaniem pozwalającym na zarządzanie pełną (maksymalną) pojemnością macierzy. Jeżeli funkcjonalność taka wymaga dodatkowych licencji, to należy je uwzględnić w ofercie.
18.	Macierz musi obsługiwać poprzez wewnętrzne mechanizmy firmware’u kopiowanie pełne (klonowanie) oraz wykonywanie min. 512 migawek (snapshotów). Jeżeli funkcjonalność taka wymaga dodatkowych licencji, to należy je uwzględnić w ofercie.
19.	Macierz musi obsługiwać poprzez wewnętrzne mechanizmy firmware’u replikację zdalną synchroniczną i asynchroniczną.
20.	Macierz musi obsługiwać QoS (Quality of Services) czyli nadawanie priorytetów obsługi transmisji I/O dla skonfigurowanych hostów, LUN-ów, portów do hostów. Jeżeli funkcjonalność ta wymaga odrębnej licencji należy dostarczyć ja wraz z macierzą w wariancie dla maksymalnej pojemności dyskowej danej macierzy.
21.	Macierz musi obsługiwać mechanizmy ograniczania wielkości pamięci podręcznej cache do obsługi wybranych woluminów LUN – tzw. cache partitioning. Jeżeli funkcjonalność ta wymaga odrębnej licencji należy dostarczyć ja wraz z macierzą w wariancie dla maksymalnej pojemności dyskowej danej macierzy oraz dla maksymalnej ilości obsługiwanych woluminów.
22.	Macierz musi posiadać funkcjonalność tieringu. Jeżeli funkcjonalność ta wymaga odrębnej licencji należy dostarczyć ja wraz z macierzą.
23.	Oprogramowanie do zarządzania macierzą musi być zintegrowane z systemem operacyjnym systemu pamięci masowej bez konieczności dedykowania oddzielnego serwera do obsługi tego oprogramowania.
24.	Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.
25.	Macierz musi posiadać wbudowaną funkcjonalność typu thinprovisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości.

4. System backupu dyskowego

Serwer backupu może być dostarczony jako jeden serwer zawierający w konfiguracji wszystkie potrzebne dyski do przechowywania danych lub jako serwer z dodatkową półką dyskową do przechowywania danych.

Producent …….....

Model …….....…...

spełniający poniższe wymagania minimalne:

2 sztuki

L.P.	Nazwa elementu	Wymagania techniczne
1.	Obudowa	Obudowa Rack 19” o wysokości maks. 3U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem kabli.
2.	Procesor	Co najmniej 2 procesory min. 6-rdzeniowe klasy x86_64 dedykowane do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 490 punktów w teście SPECint_rate_base2006 dla serwera referencyjnego z zainstalowanymi dwoma takimi procesorami. Nie wymaga się by oferowany serwer (np. producent, model) był identyczny z serwerem referencyjnym opisanym na stronie www.spec.org. Wystarczy, że posiada ten sam zestaw procesorów.
3.	Pamięć RAM	Minimum 64 GB pamięci RAM ECC Registred, serwer powinien obsługiwać co najmniej 512GB,
4.	Interfejsy sieciowe	Zainstalowane 2 porty Ethernet 1Gb/s oraz 2 porty 10Gb SFP+. Dodatkowa 2-portowa karta HBA FC 8Gb/s
5.	Kontroler	Zainstalowany sprzętowy kontroler dyskowy, posiadający min. 512MB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID : 0, 1, 5, 6, 10, 50, 60. Jeżeli opcjonalna półka dyskowa wymaga dodatkowego kontrolera powinien zostać zakupiony.
6.	Dyski twarde	Możliwość instalacji dysków twardych SATA, SAS, NearLine SAS i SSD. Liczba zainstalowanych dysków (serwer + opcjonalna dodatkowa półka) ma zapewnić backup danych źródłowych o wielkości co najmniej 20TB, Serwer powinien być wyposażony również w dodatkowe szybkie dyski na potrzeby przechowywania wewnętrznych baz i indeksów oprogramowania backupowego (np. SAS lub SSD). Dyski skonfigurowane w taki sposób aby zapewniać odporność na awarie co najmniej 2 dysków np. RAID 1, RAID 6
7.	Zasilanie	Redundantne zasilacze Hot Plug

8.	Wentylacja	Redundantne wentylatory Hot Plug
9.	Zarządzanie	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu systemu operacyjnego). Funkcjonalność przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów np. CD, USB bez konieczności dokładania dodatkowych kart

Producent …….....

Model …….....…...

Ilość ….....

spełniający poniższe wymagania minimalne:

Półka dyskowa (opcja)

L.P.	Nazwa elementu	Wymagania techniczne
1.	Obudowa	Półka dyskowa przeznaczona do instalacji w standardowej szafie rack 19” (maksymalnie 2U). Przeznaczona do podłączenia do oferowanego serwera. Półka i serwer muszą pochodzić od jednego producenta.
2.	Interfejs	Interfejs SAS 6Gbps do podłączenia kontrolerów RAID, możliwość podłączenia do 2 serwerów wraz z półką dyskową. Zamawiający wymaga dostarczenia minimum 2 kabli o długości min. 2m.
3.	Dyski	Ilość dysków odpowiednia do zapewnienia wraz z serwerem przestrzeni dla określonej wielkości backupu.
4.	Zasilanie	Redundantne zasilacze Hot Plug
5.	Wentylacja	Redundantne wentylatory Hot Plug
6.	Dodatkowe	Zainstalowany moduł umożliwiający kaskadowe podłączanie kolejnych półek dyskowych.
Wymagania funkcjonalne		
L.P.	**Funkcje**	
1.	Rozwiązanie musi reprezentować architekturę trójwarstwową (serwer zarządzający, serwer medialny oraz klient).	
2.	Rozwiązanie musi pozwalać na implementację polityki zabezpieczenia danych zorientowanej na dane, umożliwiając podejście definiujące długość życia danych w przedsiębiorstwie.	

3.	Oprogramowanie nie może preferować platformy sprzętowej, nie może być profilowane pod konkretnego dostawcą sprzętu serwerowego oraz pamięci masowych.
4.	Rozwiązanie musi zapewnić interfejs graficzny do zarządzania i instalacji.
5.	Zarządzanie systemem musi być możliwe również z przeglądarki WWW
6.	System musi zapewniać dostęp zintegrowany z usługą katalogową
7.	System musi zapewniać elastyczne delegowanie uprawnień oraz audytowanie działań użytkowników.
8.	System musi zapewniać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego tworzeniem kopii bezpieczeństwa i archiwów.
9.	System musi zapewniać funkcjonalność zdalnej instalacji modułów wykonawczych oprogramowania tworzenia kopii bezpieczeństwa i archiwów.
10.	System musi umożliwić funkcjonalność zdalnego podniesienia wersji modułów wykonawczych oprogramowania tworzenia kopii bezpieczeństwa i archiwów.
11.	System musi umożliwić przechowywanie jedynie unikalnych bloków danych tzw. deduplikacja. Funkcjonalność ta musi działać na poziomie blokowym i być wykonywana online podczas procesu tworzenia kopii lub archiwum plików.
12.	Proces deduplikacji musi być możliwy do wykonania po stronie klienckiej (serwer produkcyjny) lub serwera medialnego (serwer systemu backup obsługujący strumień danych i składujący dane).
13.	System nie może wykluczać wykorzystania urządzeń deduplikujących typu ‘appliance’ dostawców trzecich.
14.	Włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera medialnego.
15.	Oprogramowanie musi zapewnić możliwość zabezpieczenia bazy deduplikacyjnej przechowującej unikalne obiekty hash (zwany też odciskiem palca lub skrótem).
16.	Kopie i archiwa powinny być deduplikowane w oparciu o tą samą bazę skrótów.
17.	System musi umożliwiać wykonywanie kopii w post procesie do drugiej lokalizacji przesyłając jedynie unikalne bloki danych.
18.	System musi zapewniać możliwość realizacji współdzielenia obciążenia pomiędzy kilka serwerów medialnych.
19.	System musi zapewniać funkcjonalność wznawiania zadań backupowych.
20.	System musi zapewniać funkcjonalność równoległego wykonywania kopii danych (tego samego zestawu danych pojedynczego klienta) na dwa docelowe urządzenia przechowywania danych.
21.	System musi zapewniać funkcjonalność wykonywania zadania backupu wieloma równoległymi strumieniami – tzw. multistreaming.
22.	System musi zapewniać funkcjonalność multipleksowania kilku strumieni danych na nośniku

	decelowym – tzw. multiplexing.
23.	Oprogramowanie musi zapewniać mechanizm optymalizacji skanowania systemów plikowych aby skracać i minimalizować wpływ pierwszej fazy procesu tworzenia kopii lub archiwów na system produkcyjny.
24.	Rozwiązanie musi posiadać możliwość wykonywania backupu pełnego, przyrostowego, różnicowego oraz syntetycznego.
25.	System musi posiadać funkcję szyfrowania i kompresji danych transmitowanych przez LAN, możliwość wykorzystania szyfrowania i kompresji musi być dostępna w dowolnej kombinacji.
26.	System ma realizować procesy backupu oraz odzyskiwania danych.
27.	System opcjonalnie ma realizować procesy archiwizacji w trybie z oraz bez plików typu stub.
28.	Moduł archiwizujący musi być integralną częścią systemu.
29.	System ma umożliwić tworzenie zadań backupowych oraz archiwizacyjnych w oparciu o kalendarz.
30.	System musi posiadać zintegrowane w systemie mechanizmy indeksowania i wyszukiwania danych. Indeksowaniu powinny podlegać jednocześnie dane backupowane i archiwizowane
31.	System musi realizować funkcjonalność weryfikacji wykonanych kopii.
32.	System musi umożliwiać realizację szyfrowania danych po stronie klienckiej oraz serwera medialnego. Musi wspierać urządzenia taśmowe realizujące szyfrowanie danych.
33.	System musi posiadać rozbudowany system powiadamiania o zdarzeniach poprzez email oraz SNMP.
34.	System musi posiadać rozbudowany system raportowania.
35.	System powinien umożliwiać wykorzystanie funkcjonalności Bare Metal Restore.
36.	System musi umożliwiać integrację z mechanizmami kopii migawkowych czołowych producentów pamięci masowych jak np. HDS, Dell, HP, NetAPP, EMC, IBM. Integracja musi zapewnić możliwość indeksacji migawki.
37.	System musi posiadać możliwość wykonywania kopii oraz archiwów na urządzenia dyskowe
38.	System musi umożliwiać współdzielenie napędów taśmowych w sieciach SAN pomiędzy serwerami medialnymi.
39.	System musi zapewnić obsługę urządzeń taśmowych podłączanych z wykorzystaniem protokołów SAS, FC oraz IP.
40.	System powinien umożliwiać obsługę urządzeń składowania danych w chmurze.
41.	System musi umożliwiać tworzenie kopii z wykorzystaniem protokołu NDMP.
42.	System musi wspierać wykonanie kopii na systemach Windows 2003, 2008, 2012.
43.	System musi posiadać wbudowany mechanizm tworzenia kopii otwartych plików na platformie Windows.

44.	System musi wspierać wykonanie kopii na systemach klasy Linux: Ubuntu, SLES, RHEL, Debian, Fedora.
45.	System musi wspierać wykonanie kopii na systemach klasy Unix: AIX, HP-UX, Solaris.
46.	System musi umożliwiać wykonanie kopii na gorąco baz danych PostgreSQL na platformie RHEL.
47.	System musi umożliwiać wykonanie kopii na gorąco bazy danych MySQL na platformie SLES.
48.	System musi umożliwiać wykonanie kopii na gorąco bazy danych MS SQL oraz Oracle na platformie Windows.
49.	System musi umożliwiać wykonanie kopii na gorąco Active Directory a następnie odzyskania pojedynczych obiektów AD.
50.	System musi umożliwiać wykonanie kopii na gorąco aplikacji MS Exchange a następnie odzyskania pojedynczych wiadomości.
51.	System powinien umożliwiać w ramach tej samej architektury archiwizację plików na platformach systemowych Windows, AIX, HP-UX, Linux, Solaris oraz aplikacji MS Exchange i MS SharePoint. Preferowane jest rozwiązanie, w którym funkcja archiwizacji zintegrowana jest z systemem wykonywania kopii bezpieczeństwa.
52.	System musi wspierać czołowe rozwiązania wirtualizacyjne Vmware i Hyper-V.
53.	System musi wspierać najnowsze wersje środowisk VMwarevSphere 5.x poprzez integrację z vStorage API.
54.	System w kontekście platform VMware w przypadku kopii pliku VMDK musi wspierać granularne odtworzenie (odtworzenie pojedynczych plików).
55.	System musi umożliwiać backup środowisk wirtualnych poprzez integrację z mechanizmami kopii migawkowych na macierzy. Odtworzenie z migawki musi umożliwiać odzyskanie pojedynczych plików.
56.	System musi zapewniać automatyczne wykrywanie i dodawanie do polityki backupu nowych maszyn wirtualnych.
57.	System powinien umożliwiać odtwarzanie pojedynczych elementów (maili, elementów AD) z aplikacji Exchange i Active Directory zainstalowanych w środowiskach wirtualnych poprzez backup całej maszyny wirtualnej.
58.	Rozwiązanie musi w łatwy sposób skalować się horyzontalnie i wertykalnie umożliwiając łatwą rozbudowę w miarę rozrastania się infrastruktury informatycznej. Rozbudowa nie może zakłócać bieżącej pracy systemu tworzenia kopii bezpieczeństwa.
59.	Wsparcie serwisowe oraz dostęp do łat i nowszych wersji oprogramowania przez min. 36 miesięcy.

5. Oprogramowanie do zarządzania zasobami IT

Wykonawca dostarczy następujące licencje oprogramowania serwerowego:

Producent …….....

Nazwa,wersja …….....…...

spełniający poniższe wymagania minimalne:

System zarządzania infrastrukturą i oprogramowaniem musi spełniać opisane poniżej wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji.

System zarządzania komponentami musi udostępniać funkcje pozwalające na budowę bezpiecznych i skalowalnych mechanizmów zarządzania komponentami IT spełniając wymagania opisane poniżej:

4 sztuki

L.P.	Nazwa elementu	Wymagania techniczne
1.	Serwerowy system operacyjny na potrzeby wdrożenia usług katalogowych wraz z komponentami służącymi do scentralizowanego zarządzania	• Licencje pozwalające na instalowanie nieograniczonej ilości systemów operacyjnych na 4 fizycznych modułach serwerowych (po 1 licencji na moduł serwerowy), • Licencje serwerowe do scentralizowanego zarządzania nielimitowaną ilością systemów operacyjnych zainstalowanych na jednym module serwerowym (obsługującym do 2 fizycznych procesorów): zarządzanie infrastrukturą i oprogramowaniem oraz zarządzania komponentami

Załącznik nr 4 do SIWZ

Serwerowy system operacyjny powinien spełniać następujące wymagania:

Wymagania funkcjonalne	
L.P.	**Funkcje**
1	• Możliwość wykorzystania 64 fizycznych procesorów x86_64 oraz 4 TB pamięci RAM, wsparcie (na umożliwiającym to sprzęcie) dodawania pamięci RAM bez przerywania pracy. • Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy, jakości przeprowadzone przez producenta systemu operacyjnego. • Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten uwzględnia specyfikę procesorów wyposażonych w Hyper-Threading. • Wbudowane wsparcie instalacji i pracy na wolumenach, które: ◦ pozwalają na zmianę rozmiaru w czasie pracy systemu, ◦ umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, ◦ umożliwiają kompresję „w locie” dla wybranych plików lub folderów, ◦ umożliwiają zdefiniowanie list kontroli dostępu (ACL). • Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) na podstawie ich zawartość. • Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2. • Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET. • Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. • Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. • Graficzny interfejs użytkownika • Zlokalizowane w języku polskim następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. • Możliwość zmiany języka interfejsu po zainstalowaniu systemu dla języka polskiego i angielskiego. • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). • Obsługa platform sprzętowych x86, x86_64. • Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. • Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. • Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: • Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC. • Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), • Zdalna dystrybucja oprogramowania na stacje robocze. • Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej • PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: ◦ Dystrybucję certyfikatów poprzez http,

	○ Konsolidację CA dla wielu lasów domeny, ○ Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. • Szyfrowanie plików i folderów. • Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). • Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. • Serwis udostępniania stron WWW. • Wsparcie dla protokołu IP w wersji 6 (IPv6). • Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. • Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). • Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. • Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. • Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. • Zorganizowany system szkoleń i materiały edukacyjne w języku polskim w postaci samouczka dostępnego z poziomu systemu.
2	Inwentaryzacja i zarządzanie zasobami: • Inwentaryzacja zasobów serwera powinna się odbywać w określonych przez administratora systemu interwałach czasowych. System powinien mieć możliwość odrębnego planowania inwentaryzacji sprzętu i oprogramowania. • Inwentaryzacja sprzętu powinna się odbywać przez pobieranie informacji z interfejsu WMI, komponent inwentaryzacyjny powinien mieć możliwość konfiguracji w celu ustalenia informacji, o jakich podzespołach będą przekazywane do systemu. • Inwentaryzacja oprogramowania powinna skanować zasoby dyskowe przekazując dane o znalezionych plikach do systemu w celu identyfikacji oprogramowania oraz celów wyszukiwania i gromadzenia informacji o szczególnych typach plików (np. pliki multimedialne: wav, mp3, avi, xvid, itp…). • System powinien posiadać własną bazę dostępnego na rynku komercyjnego oprogramowania, pozwalającą na identyfikację zainstalowanego i użytkowanego oprogramowania. • System powinien dawać możliwość aktualizacji tej bazy przy pomocy konsoli administratora oraz automatycznie przez aktualizacje ze stron producenta. • Informacje inwentaryzacyjne powinny być przesyłane przy pomocy plików różnicowych w celu ograniczenia ruchu z agenta do serwera. Użytkowane oprogramowanie – pomiar wykorzystania: • System powinien mieć możliwość zliczania uruchomionego oprogramowania w celu śledzenia wykorzystania • Reguły dotyczące monitorowanego oprogramowania powinny być tworzone automatycznie przez skanowanie oprogramowania uruchamianego • System powinien dostarczać funkcje dystrybucji oprogramowania, dystrybucja i zarządzania aktualizacjami, instalacja/aktualizacja systemów operacyjnych. Definiowanie i sprawdzanie standardu serwera:

	• System powinien posiadać komponenty umożliwiające zdefiniowanie i okresowe sprawdzanie standardu serwera, standard ten powinien być określony zestawem reguł sprawdzających definiowanych z poziomu konsoli administracyjnej
	• Reguły powinny sprawdzać następujące elementy systemy komputerowego:
	  ○ stan usługi
	  ○ obecność poprawek (Hotfix)
	  ○ system plików
	  ○ usługi katalogowe
	Raportowanie, prezentacja danych:
	• System powinien posiadać komponent raportujący oparty o technologie webową (wydzielony portal z raportami) i/lub
	• Wykorzystujący mechanizmy raportujące dostarczane wraz z silnikami bazodanowymi
	• System powinien posiadać predefiniowane raporty w następujących kategoriach:
	  ○ Sprzęt (inwentaryzacja)
	  ○ Oprogramowanie (inwentaryzacja)
	  ○ Oprogramowanie (wykorzystanie)
	  ○ Oprogramowanie (aktualizacje, w tym system operacyjny)
	• System powinien posiadać konsolę administratora, w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu
	Analiza działania systemu, logi, komponenty:
	• Konsola systemu powinna dawać dostęp do podstawowych logów obrazujących pracę poszczególnych komponentów, wraz z oznaczaniem stanu w przypadku znalezienia zdarzeń wskazujących na problemy
	• Konsola systemu powinna umożliwiać podgląd na stan poszczególnych usług wraz z podstawowymi informacjami o stanie usługi, np. ilość wykorzystywanego miejsca na dysku twardym.

3	Architektura: • Serwery zarządzające muszą mieć możliwość publikowania informacji o uruchomionych komponentach w usługach katalogowych, informacje te powinny być odstępne dla klientów systemu w celu automatycznej konfiguracji. • Możliwość budowania struktury wielopoziomowej w celu separacji pewnych grup komputerów/usług. • System uprawnień musi być oparty o role, użytkownicy i grupy użytkowników w poszczególnych rolach powinny być pobierane z usług katalogowych. • Możliwość definiowania użytkowników do wykonywania poszczególnych zadań na klientach i serwerze zarządzającym, w tym zdefiniowany użytkownik domyślny. • Uwierzytelnianie klientów na serwerze zarządzającym przy pomocy certyfikatów w standardzie X.509, z możliwością odrzucania połączeń od klientów niezaakceptowanych. • Kanał komunikacyjny pomiędzy klientami a serwerem zarządzającym powinien być szyfrowany. • Wsparcie dla protokołu IPv6. • System powinien udostępniać funkcje autodiagnostyczne, w tym: monitorowanie stanu klientów, możliwość automatycznego lub administracyjnego restartu klienta, możliwość reinstalacji klienta. Audyt zdarzeń bezpieczeństwa - System musi udostępniać komponenty i funkcje pozwalające na zbudowanie systemu zbierającego zdarzenia związane z bezpieczeństwem monitorowanych systemów i gwarantować: • Przekazywanie zdarzeń z podległych klientów w czasie „prawie” rzeczywistym (dopuszczalne opóźnienia mogą pochodzić z medium transportowego – sieć oraz komponentów zapisujących i

	odczytujących). • Niskie obciążenie sieci poprzez schematyzację parametrów zdarzeń przed wysłaniem, definicja schematu powinna być definiowana w pliku XML z możliwością dodawania i modyfikacji. • Obsługę co najmniej 2500 zdarzeń/sek w trybie ciągłym i 100000 zdarzeń/sek w trybie „burst" – chwilowy wzrost ilości zdarzeń, jeden kolektor zdarzeń powinien obsługiwać, co najmniej 100 kontrolerów domen (lub innych systemów autentykacji i usług katalogowych) lub 1000 serwerów. Konfiguracja i monitorowanie - System musi umożliwiać zbudowanie jednorodnego środowiska monitorującego, korzystając z takich samych zasad do monitorowania różnych komponentów, a w tym: • Monitorowane obiekty powinny być grupowane (klasy) w oparciu o atrybuty, które można wykryć na klientach systemu w celu autokonfiguracji systemu. • Na podstawie wykrytych atrybutów system powinien dokonywać autokonfiguracji klientów, przez wysłanie odpowiadającego wykrytym obiektom zestawu monitorów, reguł, skryptów, zadań, itp. • System powinien posiadać możliwość monitorowania za pomocą agenta lub bez niego. • System musi pozwalać na wykrycie oraz monitorowanie urządzeń sieciowych (routery, przełączniki sieciowe, itp.) za pomocą SNMP v1, v2c oraz v3. System monitorowania w szczególności powinien mieć możliwość zbierania następujących informacji: ◦ interfejsy sieciowe ◦ porty ◦ sieci wirtualne (VLAN) ◦ grupy Hot Standby Router Protocol (HSRP) • Na podstawie uzyskanych informacji monitor powinien aktualizować status komponentu, powinna być możliwość łączenia i agregowania statusu wielu monitorów. Tworzenie reguł • w systemie zarządzania powinna mieć możliwość czerpania informacji z następujących źródeł danych: ◦ Event based (text, text CSV, NT Event Log, SNMP Event, SNMP Trap, syslog, WMI Event) ◦ Performance based (SNMP performance, WMI performance) ◦ Probe based (scripts: event, performance) • System musi umożliwiać przekazywanie zebranych przez reguły informacji do bazy danych w celu ich późniejszego wykorzystania w systemie, np. raporty dotyczące wydajności komponentów, alarmy mówiące o przekroczeniu wartości progowych czy wystąpieniu niepożądanego zdarzenia. • Reguły zbierające dane wydajnościowe muszą mieć możliwość ustawiania tolerancji na zmiany, w celu ograniczenia ilości nieistotnych danych przechowywanych w systemie bazodanowym. Tolerancja powinna mieć, co najmniej dwie możliwości: ◦ na ilość takich samych próbek o takiej samej wartości ◦ na procentową zmianę od ostatniej wartości próbki. • Monitory sprawdzające dane wydajnościowe w celu wyszukiwania wartości progowych muszą mieć możliwość – oprócz ustawiania progów statycznych, „uczenia" się monitorowanego parametru w zakresie przebiegu bazowego „baseline" w zadanym okresie. • System musi umożliwiać blokowanie modyfikacji zestawów monitorujących oraz definiowanie wyjątków na grupy komponentów lub konkretne komponenty w celu ich odmiennej konfiguracji. • System musi posiadać narzędzia do budowania modeli aplikacji rozproszonych (składających się z wielu wykrytych obiektów), pozwalając na agregację stanu aplikacji oraz zagnieżdżanie aplikacji. • Z każdym elementem monitorującym (monitor, reguła, alarm, itp.) powinna być skojarzona baza wiedzy, zawierająca informacje o potencjalnych przyczynach problemów oraz możliwościach jego

	rozwiązania (w tym możliwość uruchamiania zadań diagnostycznych z poziomu). • System musi zbierać informacje udostępniane przez systemy operacyjne Windows o przyczynach krytycznych błędów (crash) udostępnianych potem do celów analitycznych. • System musi umożliwiać budowanie obiektów SLO (Service Level Object) służących przedstawianiu informacji dotyczących zdefiniowanych poziomów SLA (Service Level Agreement) przynajmniej dla: monitora (dostępność) i licznika wydajności (z agregacją dla wartości – min., max., śr.). Przechowywanie i dostęp do informacji: • Wszystkie informacje operacyjne (zdarzenia, liczniki wydajności, informacje o obiektach, alarmy, itp.) powinny być przechowywane w bazie danych operacyjnych. • System musi mieć co najmniej jedną bazę danych z przeznaczeniem na hurtownię danych do celów historycznych i raportowych. Zdarzenia powinny być umieszczane w obu bazach jednocześnie, aby raporty mogłyby być generowane na podstawie najświeższych danych. • System musi mieć osobną bazę danych, do której będą zbierane informacje na temat zdarzeń security z możliwością ustawienia innych uprawnień dostępu do danych tam zawartych (tylko audytorzy). • System powinien mieć zintegrowany silnik raportujący niewymagający do tworzenia raportów używania produktów firm trzecich. Produkty takie mogą być wykorzystanie w celu rozszerzenia tej funkcjonalności. • System powinien mieć możliwość generowania raportów na życzenie oraz tworzenie zadań zaplanowanych. • System powinien umożliwiać eksport stworzonych raportów przynajmniej do następujących formatów: XML, CSV, TIFF, PDF, XLS, Web archive Konsola systemu zarządzania: • Konsola systemu musi umożliwiać pełny zdalny dostęp do serwerów zarządzających dając dostęp do zasobów zgodnych z rolą użytkownika korzystającego z konsoli. • System powinien udostępniać dwa rodzaje konsoli: ◦ w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu (konsola zdalna) ◦ w postaci web'owej dla dostępu do podstawowych komponentów monitorujących z dowolnej stacji roboczej (konsola webowa). • Konsola musi umożliwiać budowanie widoków tablicowych (dashboard) w celu prezentacji różnych widoków na tym samym ekranie. • Widoki powinny mieć możliwość filtrowania informacji, jakie się na nich znajdą (po typie, ważności, typach obiektów, itp.), sortowania oraz grupowania podobnych informacji, wraz z możliwością definiowania kolumn, jakie mają się znaleźć na widokach „kolumnowych". • Z każdym widokiem (obiektem w tym widoku) powinno być skojarzone menu kontekstowe, z najczęstszymi operacjami dla danego typu widoku/obiektu. • Konsola musi zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym: ◦ opcji definiowania ról użytkowników ◦ opcji definiowania widoków ◦ opcji definiowania i generowania raportów ◦ opcji definiowania powiadomień ◦ opcji tworzenia, konfiguracji i modyfikacji zestawów monitorujących ◦ opcji instalacji/deinstalacji klienta • Konsola musi pozwalać na pokazywanie obiektów SLO (Service Level Object) i raportów SLA

	(Service Level Agreement) bez potrzeby posiadania konsoli i dostępu do samego systemu monitorującego, na potrzeby użytkowników biznesowych (właścicieli procesu biznesowego). Wymagania dodatkowe: • System musi dostarczać API lub inny system (web service, connector) z publicznie dostępną dokumentacją pozwalający m.in. na: ◦ Budowanie konektorów do innych systemów, np. help-desk w celu przekazywania zdarzeń czy alarmów (dwukierunkowo), ◦ Wykonywanie operacji w systemie z poziomu linii poleceń, ◦ Podłączenie rozwiązań firm trzecich pozwalających na monitorowanie w jednolity sposób systemów informatycznych niewspieranych natywnie przez system zarządzania, ◦ Podłączenie do aplikacji biurowych pozwalające na integrację statycznych modeli z monitorowanymi obiektami, pozwalające na wyświetlanie ich stanu na diagramie.

Wykonawca dostarczy następujące licencje oprogramowania dostępowego:
Producent …….....

Nazwa,wersja …….....…...

spełniający poniższe wymagania minimalne:

1 komplet

L.P.	Nazwa elementu	Wymagania techniczne
1.	Licencje dostępowe do serwerowego systemu operacyjnego	Licencje pozwalające na dostęp do serwerowego systemu operacyjnego dla 8000 stacji końcowych (komputery, drukarki, itd.) uzyskujących dostęp do usługi katalogowej (licencjonowanie „na urządzenie”).

Załącznik nr 4 do SIWZ

Zestawienie cen:

Etap I

Nazwa	J.m.	Cena jednostkowa brutto[zł]	Cena brutto [zł] (2 x 3)
1	2	3	4
Serwer blade (wraz z systemem wirtualizacji)	1 szt.		
Macierz dyskowa podstawowa w PCPD	1 szt.		
Macierz dyskowa zapasowa w ZCPD	1 szt.		
Oprogramowanie do zarządzania zasobami IT (wytyczne odnośnie konfiguracji profili dla certyfikatów, wykonanie projektu, wdrożenie systemu, licencje serwerowe i dostępowe)	1 kompl.		
		Razem Etap I:	
		w tym podatek VAT podać w procentach	%

Etap II i III

Nazwa	J.m.	Cena jednostkowa brutto[zł]	Cena brutto [zł] (2 x 3)
1	2	3	4
System backupu dyskowego	2 szt.		
		Razem Etap II i III:	
		w tym podatek VAT podać w procentach	%

Cena oferty = Cena brutto Etap I + Cena brutto Etap II i III

Cena oferty = …..... zł brutto

.....
(pieczęć i podpis lub czytelny podpis osoby uprawnionej
do składania oświadczeń woli w imieniu Wykonawcy)